ESCUELA POLITECNICA DEL EJÉRCITO

DEPARTAMENTO DE ELECTRICA Y ELECTRONICA
CARRERA DE INGENIERIA EN ELECTRONICA, REDES Y COMUNICACIÓN DE DATOS

PROYECTO DE GRADO PARA LA OBTENCION DEL TITULO EN INGENIERIA

DISEÑO E IMPLEMENTACION DE UNA HONEYNET PARA LA RED DEL DEPARTAMENTO DE ELECTRICA Y ELECTRONICA (DEEE) UTILIZANDO VIRTUALIZACION

AUTORES

ANDREA ALBAN
CRISTIAN PALACIOS C.

SANGOLQUI – ECUADOR

2011

AGRADECIMIENTO

La presente Tesis es un esfuerzo en el cual, directa o indirectamente, participaron varias personas. En primer lugar a nuestras familias quienes nos apoyaron no solo económicamente sino también dándonos fuerzas para seguir adelante, al Ing. Carlos Romero Director de Tesis y al Ing. Fabián Sáenz Codirector de Tesis por ayudarnos con mucha paciencia en la elaboración de esta tesis y a nuestros amigos que aportaron con su conocimiento para la realización de este proyecto.

Agradecimientos sinceros.

DEDICATORIA

A mis padres, hermanos, familiares y amigos

A Uvita Cuadrado Parra

PROLOGO

El presente trabajo, comprende el diseño e implementación de una Honeynet Virtual para el Departamento de Eléctrica y Electrónica. Previamente se deberá hacer un estudio detallado del funcionamiento de la red del departamento con el fin de conocer cuáles son los puntos críticos que esta posee. Esta información permite conocer cuáles son los servicios que deberán ser comprometidos. El fin de esta implementación es descartar todos los falsos positivos y alertar de manera correcta al administrador de la red si se está produciendo un ataque, para ello se hará uso del Correlacionador de eventos SEC.

INDICE DE CONTENIDO

CAPITULO 1

MARCO TEORICO

ANTECEDENTES

En la actualidad, es de conocimiento general que el principal activo de una empresa es la información que esta posee. Debido a la sistematización del mundo, la información cada vez es más pretendida, y por ende se encuentra más propensa a ataques causados por ajenos, que aprovechan las vulnerabilidades que poseen las redes informáticas, para apoderarse de la información. Por tanto, la seguridad de la información se ha convertido en un componente crítico de la estrategia de negocio de cualquier organización.

La ESPE, al ser una institución de educación superior que maneja un flujo continuo de datos referentes a todas las actividades de la universidad, necesita garantizar la consistencia de la red, permanencia de los recursos informáticos y la seguridad de los datos que transitan a través de su red de datos, con el fin de evitar las pérdidas o alteraciones indebidas de la información.

La existencia de vulnerabilidades dentro de una red informática, implica amenazas cuya consecución son los ataques. Las vulnerabilidades pueden ser aprovechadas, con diversos fines, por muchas clases de atacantes: expertos o aficionados; interesados en el recurso de información que piensan comprometer, o motivados por intenciones en contra de la organización que atacan [1]. En los últimos años, la frecuencia de aparición de ataques ha crecido considerablemente. Este hecho, unido a las vulnerabilidades, descubiertas o latentes, en todo tipo de sistemas operativos y aplicaciones, convierte a cualquier organización en una víctima potencial. Este panorama plantea la necesidad de disponer de instrumentos que permitan descubrir y analizar las brechas de seguridad que pueda presentar un sistema, así como las técnicas y herramientas utilizadas por los posibles atacantes. Es por ello que es importante determinar las vulnerabilidades de una red

informática, para poder aplicar medidas que eviten la explotación y uso inapropiado de la red, así también conocer los métodos y técnicas más comunes para atacar a los servicios de red, con el fin de implementar medidas para bloquearlos usando dispositivos de detección y bloqueos de ataques en la red.

Un problema que no puede ser controlado por la institución es la existencia de personas, grupos de personas, organizaciones, tanto internas como externas a la institución, que trabajan diariamente en búsqueda de vulnerabilidades en Sistemas Operativos, aplicaciones informáticas, servidores y redes de computadores [2].

Es importante señalar que el principal problema de emplear un sistema de detección de ataques para la seguridad en la red, reside en que la detección y captura de actividad blackhat[1], lo que supone una sobrecarga de información [3]. Una de las labores más complicadas que se genera para las organizaciones que emplean estos sistemas, es lograr determinar de entre una gran cantidad de información, qué es tráfico productivo y qué es actividad maliciosa.

Los diferentes problemas de seguridad informática, han causado que las empresas cada vez aumenten más su interés respecto a la seguridad en la red, implementado varios mecanismos de defensa, como son: firewalls, sistemas de detección de intrusos (IDS), redes privadas virtuales (VPNs), listas de control de acceso, etc. Con esto intentan disminuir el nivel de inseguridad de la red. Además buscan implementar medios que utilizan bases de datos de marcas conocidas o algoritmos, para determinar qué es tráfico de producción y qué es actividad maliciosa [4]. Sin embargo, la sobrecarga de información, la contaminación de los datos, actividades no descubiertas, falsos positivos y falsos negativos pueden hacer el análisis y la determinación de las actividades algo extremadamente difícil.

JUSTIFICACIÓN

Debido a las vulnerabilidades y brechas de seguridad, se busca implementar una solución que permita contrarrestar los problemas de seguridad informática. Por ello, para

[1] Blackhat.- individuos con interés en atacar un sistema informático para obtener beneficios de forma ilegal.

la prevención o mitigación de cualquier tipo de amenaza es necesario conocer y comprender las vulnerabilidades constitutivas 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.

Las Honeynets son arquitecturas cuyo propósito es crear una red altamente controlada, donde sea posible capturar toda la actividad que en ella existe. Estas presentan una mejor alternativa al problema ya que estaríamos implementando un sistema que permita detectar en tiempo real actividades que puedan resultar dañinas, ya que es un recurso utilizado como carnada con el objetivo de atraer a los atacantes, destinado a capturar información extensa sobre ataques, con sistemas, aplicaciones y servicios reales a ser comprometidos (los cuales no se encuentran en producción), permitiéndonos así conocer el comportamiento y las técnicas reales que utilizan los hackers en un entorno "real". Todo el tráfico que ingrese o salga de la Honeynet será analizado utilizando la herramienta SEC (es una plataforma de código abierto y herramientas de correlación de eventos independientes), la cual nos permitirá gestionar la información obtenida en base a patrones, lo que permite diseñar alarmas a medida en función de las alertas que se vayan generando.

El diseño e implementación de esta red nos permitirá identificar las vulnerabilidades asociadas a la seguridad de la información que viaja dentro de la red del Departamento y, por otro lado, entender la importancia de definir políticas, procedimientos y estándares, de acuerdo a los requerimientos de la institución, basados en recomendaciones a nivel internacional. Además que al tratarse de una red virtual nos permitirá obtener una baja inversión en lo referente a recursos que se van a utilizar para la implementación.

1.1 Análisis del Estado de Arte

1.1.1 Introducción

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, 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 del ámbito de la red real en casos futuros.

El presente trabajo consiste en implementar un tipo especial de Honeypot denominado “Honeynet” con el objetivo es 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 con los que se cuenta en la red.

El concepto en el que se centran las Honeynets es que nos permiten estar un paso adelante del enemigo, permitiéndonos 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 [5].

1.1.2 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" [1]. 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.

1.1.2.1 Tipos de Honeypots

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

- **Honeypot de Producción**:

Llamados así por su ubicación junto a la red de producción en una organización, 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.

- **Honeypot de Investigación:**

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 sólo de capturar información para ser analizada.

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"[2], 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 sólo muestra quizá lo que sería uno de sus primeros para el ataque. 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 den ataque [6].

[2] Plug and Play.- es la tecnología que permite a un dispositivo informático ser conectado a un ordenador sin tener que configurar mediante jumpers o software específico

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

- **Honeypots físicos**

Los Honeypots Físicos son implementados en una máquina física real, lo que lo convierte en un Honeypot de alta interacción el cual puede ser comprometido totalmente. Como constituyen una máquina real, normalmente son más caros y complejos en su implementación.

- **Honeypots virtuales**

Las Honeynets virtuales consisten en combinar todos los elementos físicos de una Honeynet dentro de una única computadora, utilizando para ello software de virtualización, es decir dentro de una máquina física se levantan los Honeypots como máquinas virtuales formando la Honeynet Virtual.

- **Tipos de Honeynet virtual**

Existen dos tipos de Honeynets virtuales: las denominadas “autocontenidas” y las híbridas:

  - **Honeynets autocontenidas:** Todos sus dispositivos son virtualizados dentro de la misma máquina física.

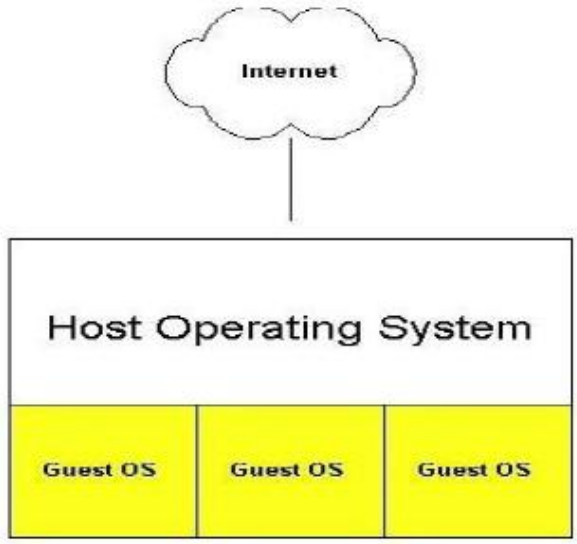


Figura. 1.1. Honeynet Virtual Autocontenida

Ventajas

- Movilidad: pueden ser instaladas en un portátil y llevadas a cualquier parte.
- Plug and Play: fácilmente pueden ser conectadas dentro de una red o de otra, ya que la implantación es fácil por ser un solo dispositivo.
- Económica: ahorra dinero porque no necesita de varios equipos, y ahorra espacio al usar un dispositivo.

Desventajas

- Punto único de fallo: si falla el hardware toda la Honeynet queda sin funcionar.
- Máquina potente: es necesario un computador potente para simular una red grande con muchos dispositivos.
- Seguridad: como se comparten dispositivos físicos como discos duros y unidades, es posible que el atacante pueda acceder a otras partes del sistema. La seguridad depende del software de virtualización.
- Hardware utilizado: limita la cantidad de sistemas operativos a simular.

- **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.

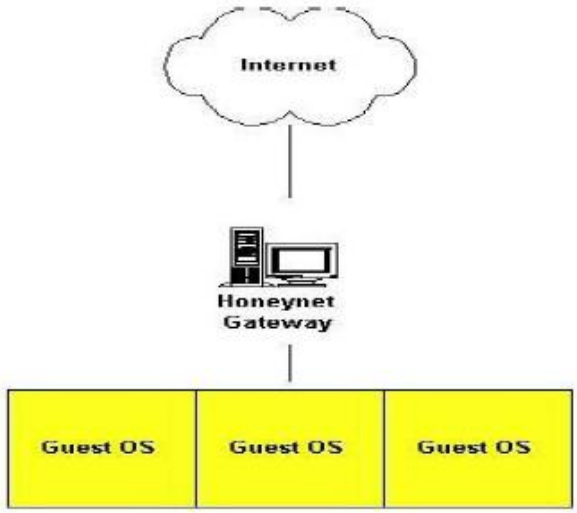


Figura. 1.2. Honeynet Virtual Híbrida

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.

Desventajas

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

1.1.2.2 Arquitectura de las Honeynets

- **Honeynets de generación I**

Fue la primera arquitectura desarrollada la Honeynet Project en 1999 y se mantuvo hasta finales del año 2001. Se compone de una máquina Gateway[3] (llamada firewall[4]) 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.

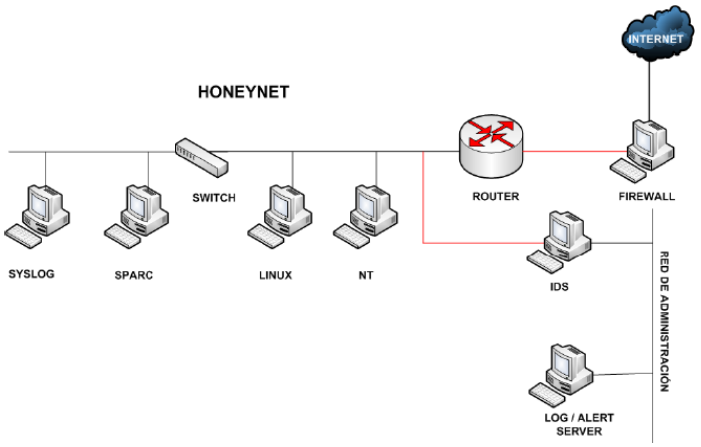


Figura. 1.3. Honeynet de Generación I

Como se muestra en la Figura 1.3, 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[5], todas las conexiones desde y para la Honeynet pasan a través de esta máquina Gateway.

La interfaz de administración simplemente se usa para configuraciones y recolección de logs en el firewall. El dispositivo IDS/Sniffer[6] posee dos interfaces, una posee una dirección IP y es utilizada para el manejo y recolección de datos. Y la otra no

[3] Gateway.- Una Pasarela o puerta de enlace es un dispositivo, que permite interconectar redes.
[4] Firewall.- Es un sistema de defensa que se basa en la instalación de una "barrera" entre tu PC y la Red.
[5] Logs.- es un registro de actividad de un sistema

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.

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:

- 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.

- **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:

- **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.

- **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 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.

- **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.

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**[7]: 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).

[7] Host.- Ordenador que permite a los usuarios comunicarse con otros sistemas centrales de una red.

- **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.

- **Honeynets de generación II**

Es la segunda arquitectura que se lanzó a principios del 2002 por el Honeynet Project. Con respecto a la arquitectura anterior 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.

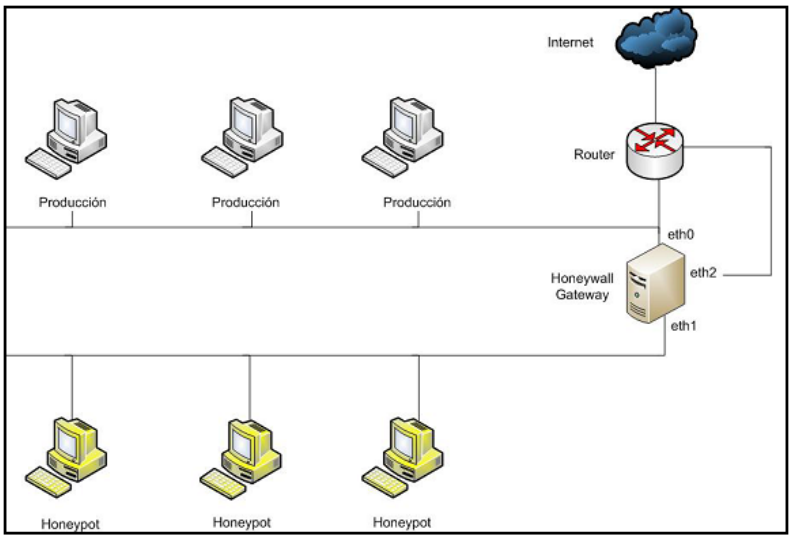


Figura. 1.4. Honeynet Generación II

En la Figura. 1.4, 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. Honeywall es el componente más crítico de toda la arquitectura posee 3 interfaces de red, donde se conectan: la red de producción, la Honeynet y la interfaz de administración.

- **Control de datos**

Todo el tráfico que circula por la Honeynet atraviesa el Honeywall, permitiendo así la intervención del firewall y de los componentes **IDS (**Sistema de Detección de intrusos**)** sobre los datos que viajan por la red.

La primera capa de control, consiste en el manejo de las conexiones salientes a través del firewall, permitiendo conexiones hasta llegar a un umbral determinado, a diferencia de las Honeynets de Gen I que sólo permitían valores muy bajos, lo cual hacía muy corta la permanencia del atacante. Mientras que la segunda capa de control de datos está conformada por el IDS.

Las dos capas se complementan con el fin de proveer de las siguientes características a la Honeynet: Limitación y control de la actividad que realizarán los atacantes dentro de la Honeynet, la forma en la que esta configuración da la apariencia de "libertad" a los atacantes que están dentro de ella lo que permitirá aprender más sobre el ataque.

Tanto la capa de control a nivel de puerta de enlace de la red como la capa de IDS implementadas en el Honeywall, pueden operar en los siguientes modos:

- **Limitación de la tasa de conexión**: Utilizando un firewall y configurándolo para prevenir exceso en el número de conexiones salientes desde cada uno de los honeypots intervinientes. Por ejemplo: limitando el número de conexiones a cierto número por hora.

- **Rechazo de paquetes**: Es un método mucho más inteligente debido a que está basado en el rechazo selectivo de paquetes maliciosos. Éste toma lugar dentro de la segunda capa si se estuviese utilizando IPS.

- **Reemplazo de paquetes**: Es un método de protección adicional, basado en IPS, para detectar o disuadir ataques. De manera que, los paquetes no son eliminados, pero se les efectúan cambios con el propósito de dejarlos inofensivos [3].

- **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.

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.

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.

- **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. 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 datos y al no poseer un API[8] que facilite la tarea de análisis. Cada fuente de datos tiene un formato independiente, todo esto simplemente retrasaba la tarea de investigación, por estas razones nace un nuevo requisito, el análisis de datos.

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 [7].

Si un atacante supera el límite de conexión usando SSH[9], 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.

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[10], SEC[11], etc.

1.1.2.3 Ventajas y desventajas de implementar Honeynets

Las Honeynets ofrecen una fortaleza muy poderosa, pero al mismo tiempo se tiene cierto nivel de riesgo, es por ello que es de vital importancia la protección que se debe implementar para nuestra red real. Entre sus principales ventajas tenemos:

[8] API.- Aplicaciones de Interfaces de Programación
[9] Ssh.- Conexión remota encriptada
[10] Sebek.- Es una herramienta diseñada para capturar datos.

- **Nuevas Herramientas y Tácticas:** Son diseñados para capturar cualquier tipo de tráfico que interactúa con ellos, incluyendo herramientas o tácticas nunca vistas.

- **Mínimos Recursos:** Los recursos pueden ser mínimos y aun así se logra implementar una plataforma potente para operar a gran escala. Ejemplo: Una computadora con un procesador Pentium con 128 Mb de RAM puede manejar fácilmente una red de clase B entera.

- **Encriptación en IPv6:** Trabaja en entornos sobre IPv6, por lo que se detectará un ataque sobre IPv6 de la misma forma que lo hace con un ataque sobre IPv4.

- **Información:** Pueden recopilar información de manera detallada a diferencia de otras herramientas de análisis de incidentes de seguridad.

- **Simplicidad:** Debido a su arquitectura, son conceptualmente simples. No existe razón por la cual se deba desarrollar o mantener nuevos algoritmos, tablas o firmas. Mientras más simple sea la tecnología, habrá menos posibilidades de error [9].

Las Honeynets también tienen debilidades propias su diseño y funcionamiento. Esto se debe a que éstos no reemplazan a las tecnologías actuales, sino que trabajan con las tecnologías existentes:

- **Visión Limitada:** Solo pueden rastrear y capturar actividad destinada a interactuar directamente con ellos. No capturan información relacionada a ataques destinados hacia sistemas vecinos, a menos que el atacante o la amenaza interactúe con el Honeypot al mismo tiempo.

- **Riesgo:** El uso de todas las tecnologías de seguridad implican un riesgo potencial. Los Honeypots no son diferentes ya que también corren riesgos, específicamente el

de ser secuestrados y controlados por el intruso y ser utilizados como plataforma de lanzamiento de otros ataques.

1.1.3 Herramientas de la Honeynet

1.1.3.1 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.

- **Snort:** Snort es un Sistema de detección de intrusiones de red, open source[12], 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.

1.1.3.2 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

[12] Open Source.- Codigo Abierto

grupos de eventos que ocurren dentro de un mismo intervalo de tiempo redefinido. SEC es un correlacionador de eventos ligero que se ejecuta como un proceso único y sigue la filosofía UNIX.

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.

- **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.

- **Opciones de Ejecucion:** Para la ejecución de perl sec.pl, se requiere emplear ciertas opciones. Entre las cuales se tienen:

"-conf=<conffile pattern>" and "-input=<inputfile>"

-conf=<file pattern>: Opción para añadir un archivo (escrito en Perl) y leer las reglas de correlación de eventos de este archivo. Múltiples opciones-conf pueden ser especificadas en la línea de comandos.

-input=<file pattern>[=<context>]: Opción para añadir un archivo (escrito en Perl) y usar el archivo como fuente de eventos. Un archivo de entrada puede ser un archivo ordinario, un archivo de logs (como se emplea en el proyecto) o entradas estándar si fueran especificadas. Múltiples opciones **–input** pueden ser especificadas en la línea de comandos. Este archivo fuente de eventos, interactúa con el archivo definido en la opción -conf, comparando que cumpla las reglas de correlación.

-testonly: Esta opción permite determinar si los archivos de la opción –conf, no contienen reglas definidas erróneamente.

- **Patrones y Tipo de Patrones**

El proyecto emplea el siguiente tipo de patrones de SEC (si <number> se omite, se asume como 1).

RegExp[<number>]: Se asume al patrón como una expresión regular, donde un número (<number>) de las últimas líneas de entrada van a ser comparadas con el patrón. En el caso de las reglas definidas en el proyecto, se ha utilizado este tipo de patrón, sin especificar <number> (number = 1), para que asume solamente el ultimo log que se recibe en el archivo fuente de eventos.

- **Listas de Acciones y Variables**

La lista de acciones consiste en la definición de las acciones a realizarse por cada regla. Se puede definir varias acciones, basta separarlas con **";"**. Cada definición de una acción empieza con una palabra clave seguida de un parámetro. Los parámetros que se puede emplear, (no necesariamente se utiliza parámetros constantes) pueden contener variables especiales de la forma: $<number> and %<number>. Los siguientes parámetros, pueden ser empleados también como variables no constantes:

%s: Descripcion del Evento.
%t: Tiempo textual del sistema (date).
%u: Tiempo numérico del sistema (time).

Cada uno de los parámetros numéricos se toma del patrón y deben ser encerrados en paréntesis. El número del parámetro varía según el orden que ocupe dentro de la línea del patrón. Para invocar a cada uno y gestionarlos, se emplea la siguiente forma:

$0: es la llamada al script.
$1: es el primer parámetro que se pasa.
$2: es el segundo parámetro, etc.

Entre las acciones permitidas en SEC, se ha empleado las siguientes:

***write* <filename> [<event text>]:** Un evento de cadena <event text> y terminación de línea son escritos en el archivo <filename>, el cual puede ser un archivo regular, un

archivo de almacenamiento de logs, o una salida estándar de shellcmd, en el caso de ser especificado.

***create* [<name> [<time> [<action list>]]]:** Se crea un contexto de nombre <name> (no puede contener espacios), con un tiempo de vida especificado en <time> (debe ser un entero constante) y vacío es decir sin ningún evento almacenado.

***add* <name> [<event text>]:** Un evento de cadena <event text> es añadido al almacenador de eventos de un contexto. Cada evento es ordenado por el tiempo en que fueron añadidos. Por tanto cada evento añadido es colocado al final del contexto.

***report* <name> [<shellcmd>]:** El almacenador de eventos de un contexto es reportado, es decir, es enviado a una entrada estándar de cmd, en el orden en que fueron añadidos, cada uno en una línea diferente. si la shellcmd es omitida, los eventos son escritos en una salida estándar.

***assign* %<alnum_name> [<text>]:** El texto <text> es asignado a una variable definida %<alnum_name>. Si <text> es omitido, se asume %s como su valor por defecto.

Las reglas de SEC, no solamente permiten acciones como la ejecución de comandos shell, sino también permiten la creación y eliminación de contextos que determinan cuando una regla en particular puede ser aplicada en un momento dado; o también permiten la generación de eventos que van a actuar como entradas o eventos a ejecutarse en otras reglas. Ello permite combinar varias reglas y desarrollar complejos esquemas de correlación, realizar acciones para añadir eventos a un contexto, reportar todos los eventos asociados a un contexto, etc. Todo esto mediante el uso apropiado de las características de SEC [8].

1.1.4 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 informática, 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.

1.1.4.1 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 decrementando los costos reutilizando el mismo hardware.

Existen diversos enfoques de virtualización, aquí listaremos algunos de ellos:

- **Emulación o simulación**: la máquina virtual simula un **hardware completo**, admitiendo un sistema operativo "guest[13]" completamente diferente. Este enfoque fue muy utilizado para permitir la creación de software para nuevos procesadores antes que estuvieran físicamente disponibles.

[13] Guest.- Invitado

- **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".

- **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.

- **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.

- **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 KVM[14] para el núcleo está incluido en Linux desde la versión 2.6.20.

1.1.4.2 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 nulo tiempo de recuperación ante un incidente.

Por otro lado, las máquinas virtuales pueden contener sistemas de distinta índole: es absolutamente posible tener un servidor de virtualización, coexistiendo con diferentes tipo 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.

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.

[14] KVM.- Máquina virtual basada en el núcleo

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 [9].

1.1.4.3 Software de virtualización seleccionado

Dentro del campo la virtualización existe diversidad de alternativas tecnológicas, pero analizaremos las más importantes en el mercado:

- VMWare: Server, Workstation, Player
- Sun VirtualBox
- Red Hat Xen 3

- **VMWare:**

Es un programa que simula un sistema físico (un ordenador, un hardware) con unas características de hardware determinadas. Cuando se ejecuta el programa (simulador), proporciona un ambiente de ejecución similar a todos los efectos a un ordenador físico, con CPU, BIOS, tarjeta gráfica, memoria RAM, tarjeta de red, sistema de sonido, conexión USB, disco duro, etc.

Vmware es un virtualizador por software que permite ejecutar (simular) varios ordenadores (sistemas operativos) dentro de un mismo hardware de manera simultánea, permitiendo así el mayor aprovechamiento de recursos. No obstante, y al ser una capa intermedia entre el sistema físico y el sistema operativo que funciona en el hardware emulado, la velocidad de ejecución de este último es menor, pero en la mayoría de los casos suficiente para usarse en entornos de producción [10].

- **Enfoque de VMware de la virtualización**

VMware inserta directamente una capa de software (VMWare ESX Server) en el hardware del ordenador o en el sistema operativo host. Esta capa de software crea máquinas virtuales y contiene un monitor de máquina virtual que asigna recursos de hardware de forma dinámica y transparente, para poder ejecutar varios sistemas operativos de forma simultánea en un único ordenador físico sin ni siquiera darse cuenta. No obstante, la virtualización de un ordenador físico único es sólo el principio. VMware ofrece una sólida plataforma de virtualización que puede ampliarse por cientos de dispositivos de almacenamiento y ordenadores físicos interconectados para formar una infraestructura virtual completa.

- **Definición de las principales funcionalidades de VMWare**

En la Tabla. 1.1 vemos un resumen de las principales funcionalidades de VMWare y qué tipo de licenciamiento necesitamos:

Tabla. 1.1. Principales Funciones de Vmware

	ESXi Single Server	Essentials	Essential Plus	Standard	Advanced	Enterprise	Enterprise Plus
ESX/ESXi	ESXi Only	✓	✓	✓	✓	✓	✓
vCenter Server Compatibility	None	vCenter Server for Essentials	vCenter Server for Essentials	vCenter Server Foundation & Standard	vCenter Server Foundation & Standard	vCenter Server Foundation & Standard	vCenter Server Foundation & Standard
Cores per Processor	6	6	6	6	12	6	12
vSMP Support	4-way	4-way	4-way	4-way	4-way	4-way	8-way
Memory/Physical Server	256GB	256GB	256GB	256GB	256GB	256GB	*No license limit
Thin Provisioning	✓	✓	✓	✓	✓	✓	✓
VC Agent		✓	✓	✓	✓	✓	✓
Update Manager		✓	✓	✓	✓	✓	✓
VMSafe		✓	✓	✓	✓	✓	✓
vStorage APIs for Data Protection		✓	✓	✓	✓	✓	✓
High Availability (HA)			✓	✓	✓	✓	✓
Data Recovery			✓		✓	✓	✓
Hot Add					✓	✓	✓
Fault Tolerance					✓	✓	✓
vShield Zones					✓	✓	✓
VMotion					✓	✓	✓
Storage VMotion						✓	✓
DRS+DPM						✓	✓
**vNetwork Distributed Switch							✓
Host Profiles							✓
Third Party Multipathing							✓

La herramienta más destacada que brinda VMware es la vCenter Server que permite centralizar la gestión, automatizar las operaciones, optimizar los recursos y alta disponibilidad en los entornos de IT.

- **VirtualBox:**

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 los tres formatos de disco virtual: el propio, el de VMWare y los .vhd de Virtual PC, trabajando con ellos sin cambiarlos.
- 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 RDP[15] de Microsoft por lo que se conecta a cualqueir 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.

[15] RDP.- Remote Desktop Protocol, es un protocolo de Microsoft que permite la comunicación en la ejecución de una aplicación entre un cliente y un servidor

- **XEN:**

Es un hipervisor de código abierto que permite una mejor utilización de los servidores y la consolidación de los mismos al posibilitar que múltiples imágenes de sistemas operativos se ejecuten simultáneamente en una único servidor físico. Es la infraestructura de virtualización por software más rápida y segura existente, y ha sido adoptada por los principales fabricantes y distribuidores, incluyendo a Intel, AMD, Dell, Hewlett-Packard, IBM, Novell, Red Hat o Sun Microsystems. Xen se distribuye bajo la licencia General Public License de GNU[16] y puede descargarse gratuitamente. Entre las principales características tenemos:

- La interfaz gráfica y la integración de ingreso y salida de datos es bastante precaria. Utiliza una variación de VNC para el control de consola
- Para máquinas virtuales Linux requiere que éstas utilicen un núcleo especializado, kernel-xen. Este kernel se puede instalar de manera nativa en distribuciones Red Hat (RHEL, CentOS y Fedora).
- El rendimiento con para-virtualization es bastante bueno en términos de uso de memoria, disco y CPU.
- El uso de discos raw (acceso directo a particiones o discos) es nativo. Esto elimina una capa adicional de acceso, utilizada comúnmente para gestionar archivos como discos virtuales.
- Una característica particular de Xen es que, al utilizar para-virtualizacion, el consumo de memoria RAM disminuye en el sistema operativo host al ser asignada a una máquina virtual [12].

1.1.5 Vulnerabilidades

Las redes y sus aplicaciones, y en particular Internet, han introducido nuevas posibilidades que también implican riesgos. Éstos surgen a partir de las *vulnerabilidades* que poseen los sistemas. La existencia de vulnerabilidades involucra amenazas, lo cual dará lugar a los ataques. Las vulnerabilidades pueden ser aprovechadas, con diversos fines,

[16] GNU.- es una licencia creada cuyo objetivo es proteger la libre distribución, modificación y uso de software.

por muchas clases de atacantes: hackers[17], piratas informáticos, crackers (Black hackers), etc.; interesados en el recurso de información que piensan comprometer, o motivados por intenciones en contra de la organización que atacan. En los últimos años, la frecuencia de aparición de ataques ha crecido considerablemente. Este hecho, unido a las vulnerabilidades, descubiertas o latentes, en todo tipo de sistemas operativos y aplicaciones, convierte a cualquier organización en una víctima potencial. Es por ello que se debe hacer uso de instrumentos que permitan descubrir y analizar los agujeros de seguridad que pueda presentar un sistema, así como las técnicas y herramientas utilizadas por los posibles atacantes.

1.1.5.1 Concepto

Las vulnerabilidades son las debilidades en un sistema, permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.

Las vulnerabilidades son el resultado de bugs o de fallos en el diseño del sistema. Aunque, en un sentido más amplio, también pueden ser el resultado de las propias limitaciones tecnológicas, porque, en principio, no existe sistema 100% seguro. Por lo tanto existen vulnerabilidades teóricas y vulnerabilidades reales (conocidas como exploits[18]).

Las vulnerabilidades en las aplicaciones suelen corregirse con parches o con cambios de versión. En tanto algunas otras requieren un cambio físico en un sistema informático. Las vulnerabilidades se descubren muy seguido en grandes sistemas, y el hecho de que se publiquen rápidamente por todo internet (mucho antes de que exista una solución al problema), es motivo de debate. Mientras más conocida se haga una vulnerabilidad, más probabilidades de que existan piratas informáticos que quieren aprovecharse de ellas [13]. Algunas vulnerabilidades típicas suelen ser:

[17] Hackers.- Son intrusos que se dedican a inspeccionar redes como pasatiempo y como reto técnico
[18] Exploits.- Programa informático malicioso (malware) que intenta utilizar y sacar provecho de un bug o vulnerabilidad

- Desbordes de pila y otros buffers.
- Errores en la validación de entradas como: inyección SQL, bug en el formato de cadenas, etc.
- Secuestro de sesiones.
- Ejecución de código remoto.

1.1.5.2 Herramientas para analizar vulnerabilidades de un red

Existen diferentes herramientas para analizar vulnerabilidades de una red. Estas herramientas son muy útiles, para los administradores de red preocupados por la seguridad e integridad de su red y la información que en ella manejan.

Entre los principales analizadores se puede encontrar NESSUS y SATAN, los cuales ofrecen una amplia gama de reglas para evaluar las vulnerabilidades y además permiten la incorporación de nuevas reglas para hacer mpas riguroso y específico el análisis [14].

- **NESUS**

Es un analizador de vulnerabilidades gratuito, poderoso, actualizado y fácil de utilizar. Este programa además es extensible, robusto, seguro, de propósito general (no está limitado a un solo tipo de vulnerabilidades) y más importante que cualquier otra característica, es su amplia aceptación por la comunidad. Está basado en plug-in (s), tiene una interfaz basada en GTK[19], y realiza más de 1200 pruebas de seguridad remotas. Permite generar reportes en HTML[20], etc.; también sugiere soluciones para los problemas de seguridad.

[19] GTK.- GIMP Toolkit es un conjunto de bibliotecas multiplataforma para desarrollar interfaces gráficas de usuario (GUI)
[20] HTML.- (L*enguaje de Marcado de Hipertexto*) es el lenguaje de marcado predominante para la elaboración de páginas web.

- **SATAN**

(Security Analysis Tool for Auditing Networks, por sus siglas en inglés) es una herramienta de prueba y análisis que recolecta información variada sobre una red y los hosts que se encuentran en ella.

Esta herramienta recopila información mediante un análisis de los servicios de la red. Después, elabora un reporte, con un sistema simple de reglas en el que evidencia las vulnerabilidades de la red. Entre la información que detecta SATAN se encuentra:

- Topología de la red.
- Servicios de la red.
- Tipo de hardware.
- Tipo de software

- **N-STEALTH**

Es una herramienta que escanea servidores Web para identificar problemas y debilidades que pueden permitir que un atacante obtenga acceso privilegiado. N-Stealth tiene una base de datos con más de 30.000 vulnerabilidades y exploits. La base de datos de N-Sealth es actualizada activamente y por ende contiene más vulnerabilidades que una base normal. El lema de este software es: "*encuentre sus vulnerabilidades antes que un hacker lo haga*".

- **NIKTO – LibWhisker:**

Es un analizador de vulnerabilidades para servidores Web, basado en la funcionalidad de HTTP de la librería LibWhisker de Wiretrip. Este analizador busca malas configuraciones, software que no está al día con las actualizaciones, archivos y scripts que están por default o inseguros, los cuales colocan en alto riesgo el servidor. Es un script de

perl[21], que maneja las pruebas de las diferentes vulnerabilidades mediante plug-ins también escritos en perl. La herramienta se compone de un paquete de pruebas básicas, pero también permite la escritura de pruebas adicionales para necesidades específicas. Estas pruebas básicas cubren una amplia gama de vulnerabilidades en diferentes servidores Web y sistemas operativos.

- **ISS – INTERNET SECURITY SCANNER:**

Es una aplicación cuyo objetivo es buscar puntos vulnerables de la red con relación a la seguridad. Es una herramienta comercial de análisis de vulnerabilidades para Windows. ISS (Internet Security Scanner); siendo el utilitario comercial más popular del mercado**.** Se basa en una herramienta denominada ISS que, al igual que SATAN, salió al mercado con carácter gratuito.

1.1.6 Ataques a las redes de información

Un "**ataque**" consiste en aprovechar una vulnerabilidad de un sistema informático (sistema operativo, programa de software o sistema del usuario) con propósitos desconocidos por el operador del sistema y que, por lo general, causan un daño.
Los ataques siempre se producen en Internet, a razón de varios ataques por minuto en cada equipo conectado. En su mayoría, se lanzan automáticamente desde equipos infectados (a través de virus, troyanos, gusanos, etc.) sin que el propietario sepa lo que está ocurriendo. En casos atípicos, son ejecutados por piratas informáticos.

1.1.6.1 Fases de un Ataque Informático

Los ataques contra redes de ordenadores y sistemas informáticos suelen constar de las etapas o fases que se presentan a continuación:

1. Descubrimiento y exploración del sistema informático.

[21] Perl.- Practical Extracting and Reporting Languaje, lenguaje de programación que extrae información de archivos de texto.

2. Búsqueda de vulnerabilidades en el sistema.
3. Explotación de las vulnerabilidades detectadas (“exploits”).
4. Corrupción o compromiso del sistema: modificación de programas y ficheros del sistema para dejar instaladas determinadas puertas traseras o troyanos; etcétera.
5. Eliminación de las pruebas que puedan revelar el ataque (“logs”)

Para poder llevar a cabo un ataque estos deben disponer de herramientas y conocimientos lo que es conocido como:“Triángulo de la Intrusión”, que se ve en las siguiente figura:

Figura. 1.5. El “Triángulo de la Intrusión”

En cuanto a las herramientas (“Hacking Tools”), podríamos citar las siguientes: Escáneres de puertos, sniffers, exploits, backdoors kits[22], rootkits (ocultan “puertas traseras”), auto-rooters (automatizan un ataque, password crackers, generadores de virus y otros programas, etc.

1.1.6.2 Tipos de Ataques

Los tipos de ataques en las redes de información de una manera general se distinguen dos tipos:

- Ataques Activos: Son los que distorsionan la información y la situación de los recursos del sistema.

[22] Backdoors kits.- son un conjunto de instrucciones no documentadas, que permiten tomar el control del equipo sin importándole la seguridad

- Ataques Pasivos: registran el uso de los recursos y el acceso a la información guardada transmitida por el sistema.

Entre los principales tipos de ataques contra redes y sistemas informáticos se tiene:

- **Actividades de reconocimiento.-** No ocasionan ningún daño, su objetivo es obtener información de las redes y sistemas informáticos, para lo cual hace un escaneo de puertos para determinar qué servicios se encuentran activos y el las versiones de sistemas operativos.

- **Detección de vulnerabilidades.-** Intentan identificar y documentan las posibles vulnerabilidades de un sistema informático, para luego poder hacer uso de estas ("exploits").

- **Robo de información mediante la interceptación de mensajes.-** Interceptan los e-mial's o los documentos que se envían a través de redes de ordenadores.

- **Análisis del tráfico.-** Observan todo el tráfico transmitido a través de redes informáticas, utilizando "sniffers".

- **Ataques de suplantación de la identidad**

    - **IP Spoofing.-** El atacante altera la cabecera de los paquetes enviados a un determinado equipo, engañando que son enviados de un equipo distinto al que verdaderamente los ha originado. "Hijacking" el atacante trata de suplantar la dirección IP de la víctima y el número de secuencia del próximo paquete de datos que va a transmitir.

- **DNS Spoofing.-** Provocan un direccionamiento erróneo en los equipos afectados, debido a una traducción errónea de los nombres de dominio a direcciones IP, redireccinando a los usuarios hacia páginas Web falsas. Para lo cual el atacante hace uso de un servidor DNS legítimo para que acepte y utilice información incorrecta obtenida de un ordenador que no posee autoridad para ofrecerla, de esta manera la base de datos del servidor se llena de nombres falsos, este proceso se lo conoce como "envenenamiento de la caché del servidor DNS".

- **SMTP Spoofing.-** El envío de mensajes con remitentes falsos ("masquerading") para engañar al destinatario, los virus emplean esta técnica para facilitar su propagación.

- **Captura de cuentas de usuario y contraseñas.-**"Snooping" permite observar la actividad de un usuario en su ordenador para obtener determinada información de interés, como podrían ser sus contraseñas. Los programas que permiten realizar esta actividad son los "snoopers", los cuales pueden ser troyanos u otros "parásitos" que inspeccionan dispositivos de entrada como los ratones y los teclados.

- **Conexión no autorizada a equipos y servidores.-** Existen varias posibilidades para establecer una conexión no autorizada a otros equipos y servidores: Violación de sistemas de control de acceso, Agujeros de seguridad ("exploits"), Backdoors son un conjunto de instrucciones no documentadas, que permiten tomar el control del equipo sin importándole la seguridad, Rootkits, parecidos a los troyanos, que se instalan en un equipo reemplazando a una herramienta o servicio legítimo del sistema operativo.

- **Phishing.-** Tratan de obtener números de cuenta y las claves de acceso a servicios bancarios, para realizar con ellos operaciones fraudulentas que perjudiquen a los legítimos propietarios. Esto lo realizan utilizando una imitación de las páginas Web de los servicios bancarios que pretenden suplantar.

- **Pharming.-** hacen uso de un virus que conecta a las víctimas desde su ordenador a páginas falsas en lugar de a las legítimas correspondientes a sus propias entidades financieras.

- **Denegación del Servicio (Ataques DoS – Denial of Service).-** DoS se produce cuando un usuario que tenía permisos para acceder a un servicio y no puede hacerlo. Para ello, existen varias posibilidades de conseguirlo: "Ataque reflector" ("reflector attack"), que persigue generar un intercambio ininterrumpido de tráfico entre dos o más equipos, "El ping de la muerte": mediante el comando "ping –l 65510 direccion_equipo_victima", que envía un paquete IP de un tamaño superior a los 65.536 bytes, provocando el reinicio colapso del equipo, "Land Attack": en algunos sistemas Windows, se consigue "colgar" un equipo vulnerable mediante el envío de una serie de paquetes maliciosamente construidos, "SYN Flood": incumplimiento de las reglas básicas del protocolo TCP por parte del cliente, provocando se realicen conexiones en estado de "semi-abierta", consumiendo de este modo recursos de la máquina.

CAPITULO 2

ANALISIS DEL SISTEMA DEL DEEE

2.1 Análisis de la Red Actual

2.1.1 Análisis de Hardware y de Software.

La red del departamento de Eléctrica y Electrónica, está formado por dos servidores:

1. Firewall: Cuyo sistema operativo es Linux Centos realese 5.4, kernel 2.6.18-164.e15, que posee una memoria total de 515740, de la cual se encuentra ocupada 181956 y un espacio libre de 333784, posee tres tarjetas de red:

   a. eth0: IP: 10.1.28.2, Mascara: 255.55.252.0, MAC: 00:0C:76:5C:61:43 (FastEthernet).

Tabla. 2.1 Descripción de las subinterfaces de red eth0 del Firewall

eth0:1	10.1.28.3/22
eth0:2	10.1.28.4/22
eth0:3	10.1.28.5/22
eth0:4	10.1.28.6/22

   b. eth1: MAC:00:13:F7:48:60:6F, posee cuatro subinterfaces, es una interfaz GigabitEthernet

Tabla. 2.2 Descripción de las subinterfaces de red eth1 del Firewall

eth1:2	10.1.30.1/24	Red de Profesores
eth1:3	10.1.29.1/24	Red de Alumnos
eth1:4	192.168.1.1/24	Pruebas de Red
eth1:10	10.10.0.1/24	Red de Servidores

c. eth2: IP: 201.234.84.173, Macara: 255.55.255.25, MAC: 00:13:F7:48:6C:47 (GigabitEthernet) Salida a internet

2. Servidor Web (kyo.deee.espe.edu.ec): sistema operativo Linux Centos release 5.4, kernel 2.6.18-164.e15, que posee una memoria total de 12297884, de la cual se encuentra ocupada 4964224 y un espacio libre de 7338660, tiene una sola interfaz de red.
   a. eth0: IP: 10.10.0.2, MASCARA: 255.255.255.0, MAC:00:25:B3:AD:75:BE, posee una subinterfaz, es una interfaz GigabitEthernet

Tabla. 2.3 Descripción de las subinterfaces Servidor WEB de red eth0

Eth0:1	192.188.58.54/24	

La red física del Departamento de Eléctrica y Electrónica esta divida en diferentes bloques. Los laboratorios de Electrónica contarán con cinco bastidores, uno por cada planta, cuyas identificaciones son A1, B1, B2, C1 y C2 respectivamente. La identificación de bastidores se muestra en la figura:

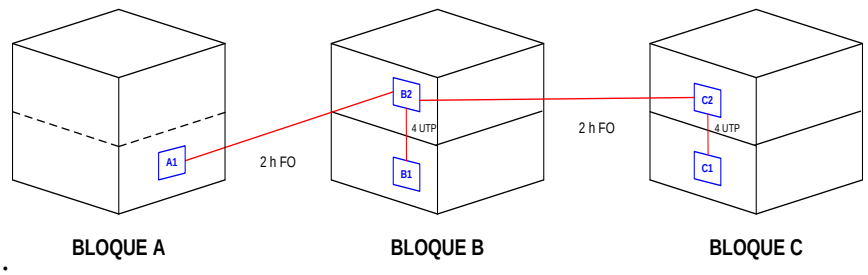


Figura. 2.1 Identificación de Bastidores

A continuación de detalla la distribución de cada rack que componen la red del DEEE, se muestra un esquema con todos los elementos que pertenecen a los rack, además se detalla cómo se encuentran interconectados cada uno de sus elementos.

- **Bloque A:**

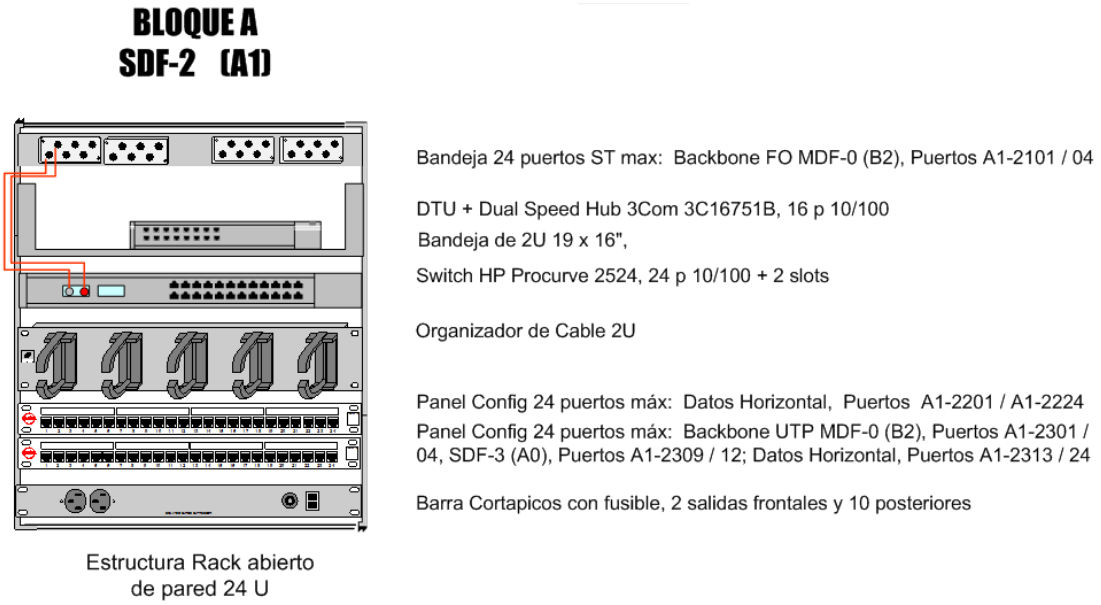


Figura. 2.2 Rack A1

La conexión entre los elementos está dispuesta de la siguiente manera:

Tabla. 2.4 Interconexión de Equipos del Rack A1 (Id: 2201-2224)

Patch Panel	Id de Canal	Swicth HP2524	Hub 3Com
1	2201	13	
2	2202	14	
3	2203	15	
4	2204	17	
5	2205	16	
6	2206	18	
7	2207	19	
8	2208	20	
9	2209	21	
10	2210	22	
11	2211	23	
12	2212	Libre	
13	2213		6
14	2214		5
15	2215		13
16	2216	Libre	
17	2217		10
18	2218		7
19	2219		14
20	2220		9
21	2221		8
22	2222	Libre	
23	2223	Libre	
24	2224	Libre	

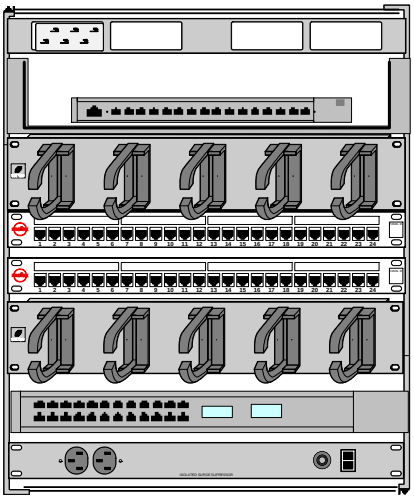
Tabla. 2.5 Interconexión de Equipos del Rack A1 (Id: 2301-2324)

Patch Panel	Id de Canal	Swicth HP2524	Hub 3Com
1	2301		
2	2302		
3	2303		
4	2304		
5	2305		
6	2306		
7	2307		
8	2308		
9	2309	12	
10	2310		12
11	2311		11
12	2312		
13	2313	2	
14	2314	3	
15	2315	4	
16	2316	5	
17	2317	6	
18	2318	7	
19	2319	8	
20	2320	9	
21	2321		
22	2322		
23	2323		
24	2324	10	

Tabla. 2.6 Interconexión de Equipos Rack A1

Swicth HP2524	Hub 3Com
11	1

- **Bloque B1**



Estructura Rack abierto de pared 12 U

HUB MicroNet UNICON, 16 puertos
Bandeja de 2U 19 x 16",

Organizador de Cable 2U

Panel 24 puertos: Backbone UTP MDF-0 (B2), Puertos B1-1201 / 04; Datos Horizontal, Puertos B1-1205 / B1-1212
Panel 24 puertos: Datos Horizontal, Puertos B1-1301 / B1-1324

Organizador de Cable 2U

Switch HP Procurve 2524, 24 p 10/100 + 2 slots

Barra Cortapicos con fusible, 2 salidas frontales y 10 posteriores

Figura. 2.3 Rack B1

La conexión entre los elementos está dispuesta de la siguiente manera:

Tabla. 2.7 Interconexión de Equipos Rack B1 (Id: 1201-1224)

Patch Panel	Id de Canal	Swicth HP2524
1	B1 1201	21
2	B1 1202	22
3	B1 1203	23
4	B1 1204	24
5	B1 1205	10
6	B1 1206	13
7	B1 1207	14
8	B1 1208	15
9	B1 1209	16
10	B1 1210	17
11	B1 1211	19
12	B1 1212	20
13	B1 1213	
14	B1 1214	
15	B1 1215	
16	B1 1216	
17	B1 1217	
18	B1 1218	
19	B1 1219	
20	B1 1220	
21	B1 1221	
22	B1 1222	
23	B1 1223	
24	B1 1224	

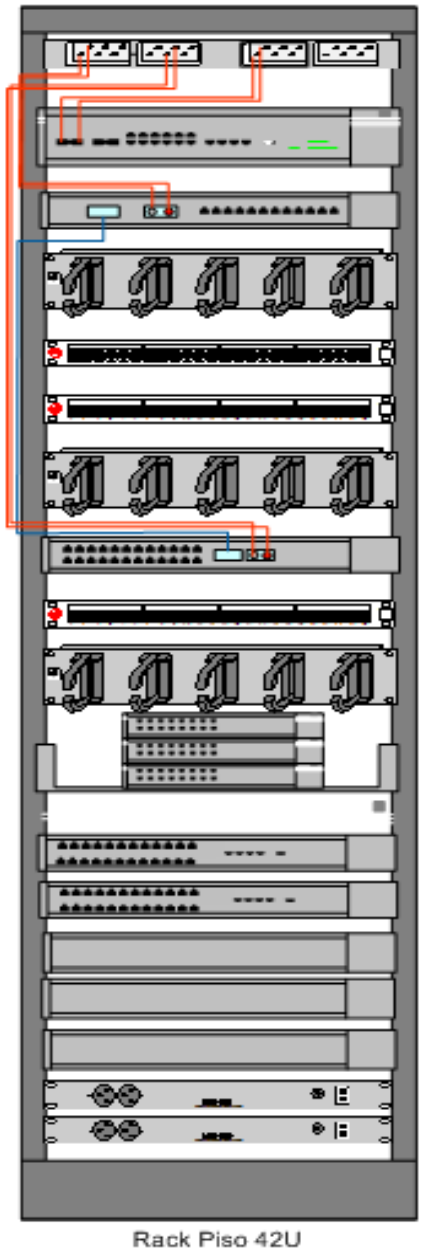
Tabla. 2.8 Interconexión de Equipos Rack B1 (Id: 1301-1324)

Patch Panel	Id de Canal	Swicth HP2524	Hub 3Com
1	B1 1301	1	
2	B1 1302	2	
3	B1 1303	3	
4	B1 1304	4	
5	B1 1305	5	
6	B1 1306	7	
7	B1 1307	8	
8	B1 1308	9	
9	B1 1309	12	
10	B1 1310		
11	B1 1311		
12	B1 1312		
13	B1 1313		
14	B1 1314		2
15	B1 1315		3
16	B1 1316		4
17	B1 1317		5
18	B1 1318		6
19	B1 1319		7
20	B1 1320		
21	B1 1321		8
22	B1 1322		9
23	B1 1323		11
24	B1 1324		

Tabla. 2.9 Interconexión de Equipos Rack B1

Swicth HP2524	Hub 3Com
11	Uplink

- **Bloque B2**



Switch HP Procurve 2512, 12 p 10/100 + 2 slots + 2 slots Staking

Organizador de Cable 2U

Panel Config 24 puertos máx: Backbone UTP SDF-1 (B1), Puertos B2-0205 / 08

Panel Config 24 puertos máx: Datos Horizontal, Puertos B2-0301 / B2-0324

Organizador de Cable 2U

Switch HP Procurve 2524, 24 p 10/100 + 2 slots

Panel Config 24 puertos máx: Datos Horizontal, Puertos B2-0401 / B2-0424

Organizador de Cable 2U

Dual Speed Hub 16 3Com 3C16751B, 16 p 10/100
Dual Speed Hub 16 C 3Com 3C16751B, 16 p 10/100
Dual Speed Hub 16 3Com 3C16751B, 16 p 10/100
Bandeja de 2U 19 x 16",

RAS 1500 E1 PRI Expansion, 3C433279A
RAS 1500Base, 3C421600A

Barra Cortapicos con fusible, 2 salidas frontales y 10 posteriores

Barra Cortapicos con fusible, 2 salidas frontales y 10 posteriores

Figura. 2.4 Rack B2

La conexión entre los elementos está dispuesta de la siguiente manera:

Tabla. 2.10 Interconexión de Equipos Rack B2 (Id: 2201-2224)

Patch Panel	Id de Canal	Swicth 3Com 4050	Switch HP 2512	Switch HP 2524
1	B2 201	11		
2	B2 202			
3	B2 203			
4	B2 204			
5	B2 205			21
6	B2 206			22
7	B2 207			23
8	B2 208			24
9	B2 209			
10	B2 210			
11	B2 211			
12	B2 212			
13	B2 213			
14	B2 214			
15	B2 215			
16	B2 216			
17	B2 217			
18	B2 218	8		
19	B2 219	7		
20	B2 220	9		
21	B2 221	17		
22	B2 222		4	
23	B2 223			
24	B2 224	13		

Tabla. 2.11 Interconexión de Equipos Rack B2 (Id: 2301-2324)

Patch Panel	Id de Canal	Switch HP 2524	Hub 2	Hub 3
1	B2 301			1
2	B2 302			2
3	B2 303			3
4	B2 304			4
5	B2 305			5
6	B2 306			6
7	B2 307			7
8	B2 308			8
9	B2 309			9
10	B2 310			10
11	B2 311			11
12	B2 312			
13	B2 313			
14	B2 314			
15	B2 315			
16	B2 316			
17	B2 317		1	
18	B2 318		2	
19	B2 319		3	
20	B2 320			
21	B2 321	19		
22	B2 322	20		
23	B2 323		13	
24	B2 324		15	

Tabla. 2.12 Interconexión de Equipos Rack B2 (Id: 2401-2424)

Patch Panel	Id de Canal	Switch HP 2524	Switch 3Com 4050	Hub 2
1	B2 401	1		
2	B2 402	2		
3	B2 403	3		
4	B2 404	4		
5	B2 405	5		
6	B2 406	6		
7	B2 407	7		
8	B2 408	8		
9	B2 409	9		
10	B2 410	10		
11	B2 411	11		
12	B2 412	12		
13	B2 413			
14	B2 414			
15	B2 415			
16	B2 416			12
17	B2 417			11
18	B2 418	14		
19	B2 419	13		
20	B2 420		2	
21	B2 421	15		
22	B2 422	16		
23	B2 423	17		
24	B2 424	18		

Tabla 2.13 Interconexión de Equipos Rack B2

Swicth 3Com 4050	Switch HP 2512	RAS	Switch 1 3Com 4500	Switch 2 3Com 4500
10			27	
11	12			
12				27
	6	LAN		

- **Bloque C1**

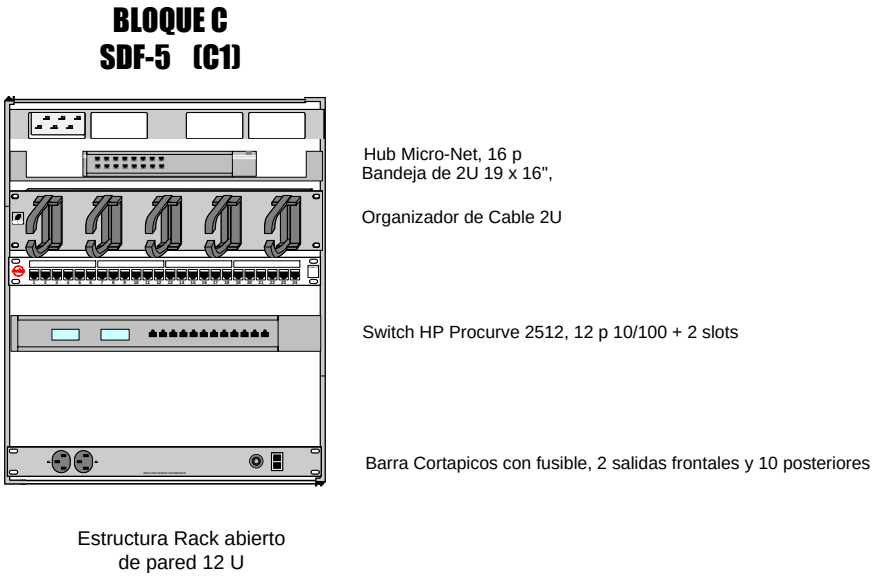


Figura. 2.5 Rack C1

La conexión entre los elementos está dispuesta de la siguiente manera:

Tabla. 2.14 Interconexión de Equipos Rack C1 (Id: 5201-5224)

Patch Panel	Id de Canal	Hub MicroNet	Switch HP 2512
1	C1 5201	7	
2	C1 5202		11
3	C1 5203		
4	C1 5204		
5	C1 5205		1
6	C1 5206		2
7	C1 5207		6
8	C1 5208	15	
9	C1 5209	14	
10	C1 5210		12
11	C1 5211		4
12	C1 5212	13	
13	C1 5213	12	
14	C1 5214	11	
15	C1 5215	10	
16	C1 5216		5
17	C1 5217		3
18	C1 5218		
19	C1 5219		
20	C1 5220		7
21	C1 5221		
22	C1 5222		8
23	C1 5223		
24	C1 5224		9

Tabla. 2.15 Interconexión de Equipos Rack C1

Swicth HP2512	Hub 3Com
10	Uplink

- **Bloque C2**

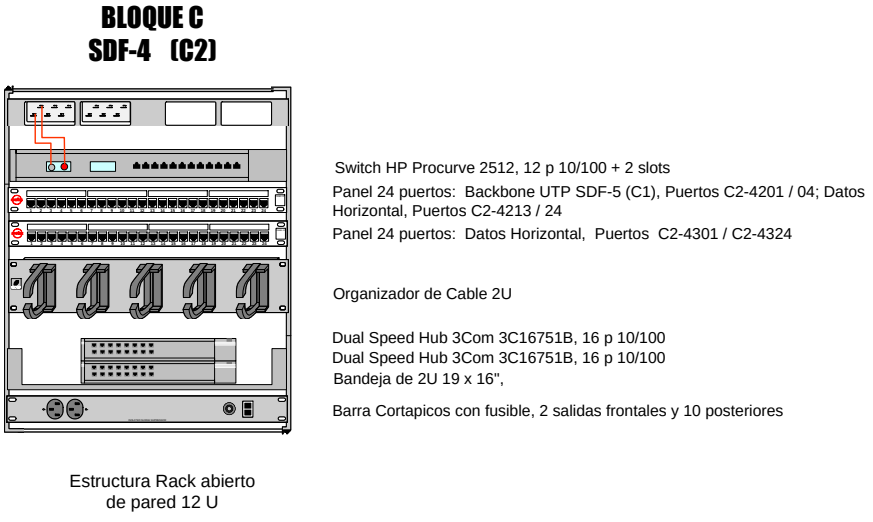


Figura. 2.5 Rack C2

Tabla. 2.16 Interconexión de Equipos Rack C2 (Id: 4201-4224)

Patch Panel	Id de Canal	Switch HP 2512
1	C2 4201	
2	C2 4202	
3	C2 4203	
4	C2 4204	
5	C2 4205	12
6	C2 4206	11
7	C2 4207	
8	C2 4208	
9	C2 4209	
10	C2 4210	
11	C2 4211	
12	C2 4212	
13	C2 4213	1
14	C2 4214	2
15	C2 4215	3
16	C2 4216	4
17	C2 4217	5
18	C2 4218	6
19	C2 4219	7
20	C2 4220	8
21	C2 4221	
22	C2 4222	
23	C2 4223	
24	C2 4224	

Tabla. 2.17 Interconexión de Equipos Rack C2 (Id: 4301-4224)

Patch Panel	Id de Canal	Hub 1	Hub 2
1	C2 4301		1
2	C2 4302		2
3	C2 4303		3
4	C2 4304		4
5	C2 4305		5
6	C2 4306		6
7	C2 4307		7
8	C2 4308		8
9	C2 4309		11
10	C2 4310		9
11	C2 4311		12
12	C2 4312		
13	C2 4313	4	
14	C2 4314	3	
15	C2 4315	2	
16	C2 4316	1	
17	C2 4317	15	
18	C2 4318	14	
19	C2 4319	11	
20	C2 4320		
21	C2 4321	13	
22	C2 4322	10	
23	C2 4323	12	
24	C2 4324	9	

Tabla. 2.18 Interconexión de Equipos Rack C2

Swicth HP2512	Hub 1	Hub 2
9		16
10	16	

2.1.2 Análisis de los Servicios.

La red presta los siguientes servicios:

1. El servidor FIREWALL presta los servicios de:
   - IPTABLES.- Define políticas aplicadas a VLANS, de NAT, ROUTE, FORWARD.
   - DHCP.- Especifica el rango de direcciones ip, desde la dirección 10.1.30.0/24 hasta la dirección 10.1.30.255/24 para la red de profesores. Y desde la dirección 10.1.29.0/24 hasta la dirección 10.1.29.255/24 para la red de alumnos.
   - DNS.- El servidor DNS que determina el dominio www.deee.espe.edu.ec para la dirección ip 10.1.28.3/22.
   - NTOP.

2. El servidor WEB presta los servicios de:
   - HTTP.- Presta servicio de página web.
   - MAIL.- Servidor de Correo Zimbra, que presa servicios SNTP[22], POP3[23], IMAP[24]
   - MySQL.

2.1.3 Análisis del tráfico de la Red.

La medición de tráfico de datos se realizó utilizando el software Fluke Networks Optiview Protocol Expert. El software fue instalado en el host 10.1.30.132 conectado al puerto 2 del Switch 1 3Com 4050 del rack B2, para realizar la captura del trafico de toda la red el Switch fue configurado como Port Mirroring (es una configuración que podemos establecer en un Switch, con el fin de que este envíe una copia de todos los paquetes que pasan por uno o más puertos (**mirroring-port**) a otro puerto concreto que llamamos **monitor-port** o, a otro Switch. [15]), el puerto 2 fue configurado de monitor port y el

[22] SNTP.- Es un servicio cliente/servidor de sincronización horaria para satisfacer los deseos de los usuarios.
[23] POP3.- Protocolo 3 de Correo Es un protocolo estándar para recibir mensajes de e-mail.
[24] IMAP.- Internet Message Access Protocol, es un protocolo de red de acceso a mensajes electrónicos almacenados en un servidor.

puerto 20 como mirroring port además que se agregaron todas la VLANS para con esto poder conectar el punto que pertenece al servidor que brinda todos los servicios.

En las siguientes figuras que fueron obtenidas mediante el software Fluke Networks nos permiten determinar las especificaciones del tráfico que circula por la red.

La figura 2.6, nos permite conocer el porcentaje de tráfico en frames, por cada protocolo. Se puede observar que el mayor tráfico que circula por la red es OTHERS (consiste en otros protocolos como CDP, ETHERNET, NMB, etc.). A continuación de OTHERS, protocolo que más circula por la red es el HTTP.

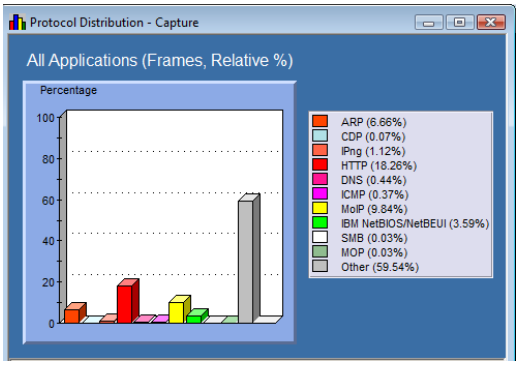


Figura. 2.6 Captura de la Distribución por Protocolo

En la figura. 2.7 se puede observar el tamaño de los paquetes, en bytes, que más circulan en la red, es entre 1024 -1516 kbps.

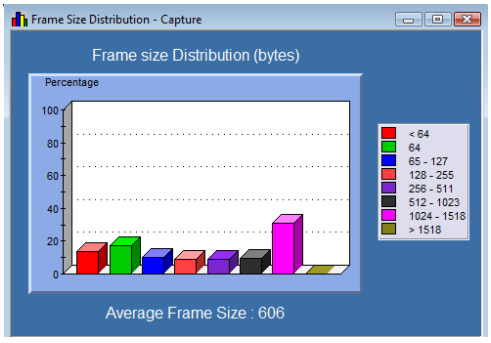


Figura. 2.7 Tamaño de la Distribución de Paquetes

En la figura. 2.8, muestra los 10 equipos que reciben la mayor cantidad de tráfico, en frames, dentro de la red. Aquí podemos determinar que el equipo que recibe mayor tráfico es el 10.1.30.196, que pertenece a la red de profesores. El siguiente equipo que recibe mayor cantidad de frames, es el 10.1.0.112 que corresponde al servidor de nombre serverisa.espe.int.

La figura 2.9 muestra, los mismos equipos pero indicando el respectivo tipo de aplicación

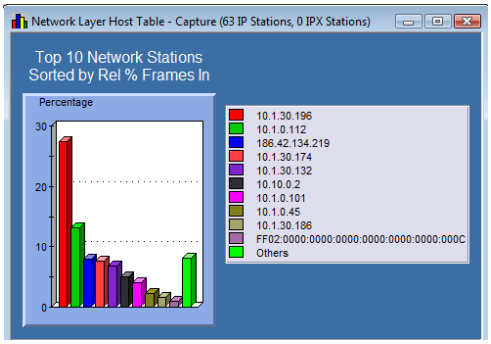


Figura. 2.8 Equipos que reciben la mayor cantidad de tráfico en frames.

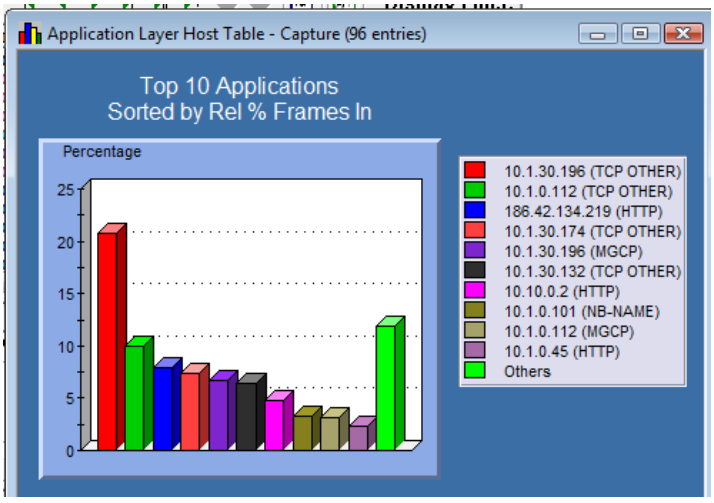


Figura. 2.9 Equipos que reciben la mayor cantidad de tráfico y su aplicación.

En la figura 2.10 se puede apreciar que los equipos que más tráfico comparten, son el host 10.1.30.196 y el servidor 10.1.0.112, que anteriormente fueron descritos. La figura 2.11 permite observar que tipo de aplicación es la que se manejan entre estos equipos.

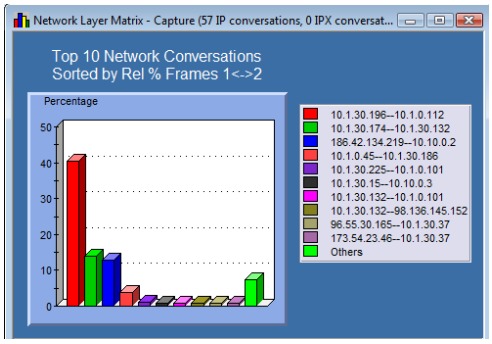


Figura. 2.10 Equipos que comparten más tráfico.

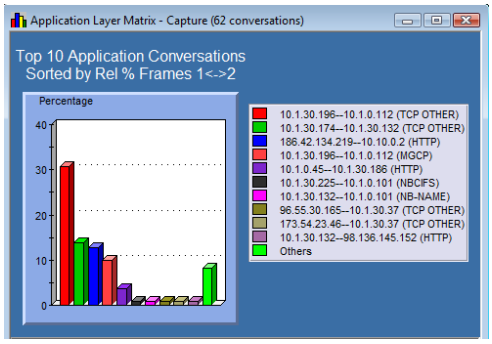


Figura. 2.11 Equipos que comparten más tráfico y su aplicación.

2.1.4 Tipo de Topología Física y Lógica

- **Topología Física**

La Topología Física de la red LAN en el departamento de Eléctrica y electrónica, consta de un servidor conectado en estrella a los diferentes terminales. En la figura 2.12 se indica la distribución de los equipos conectados.

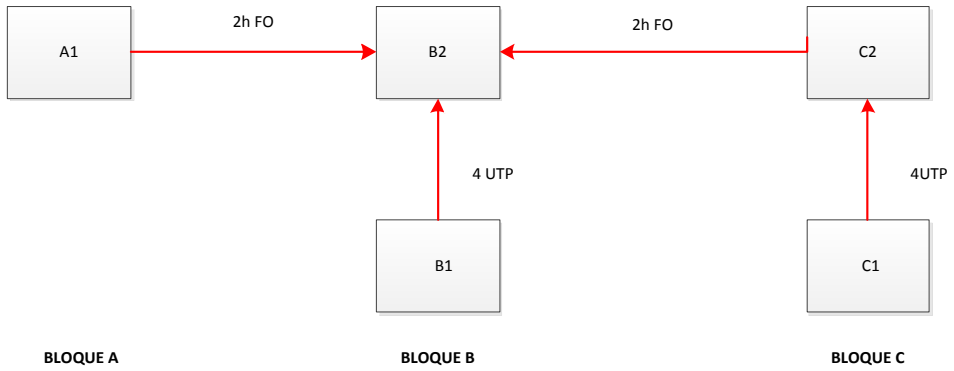


Figura. 2.12 Topología Física del DEEE

- **Topología Lógica**

El diseño de la topología lógica de la red del Departamento de Eléctrica y Electrónica, hace referencia al direccionamiento empleado para completar el diseño de la topología física, como se puede observar en la Figura. 2.12

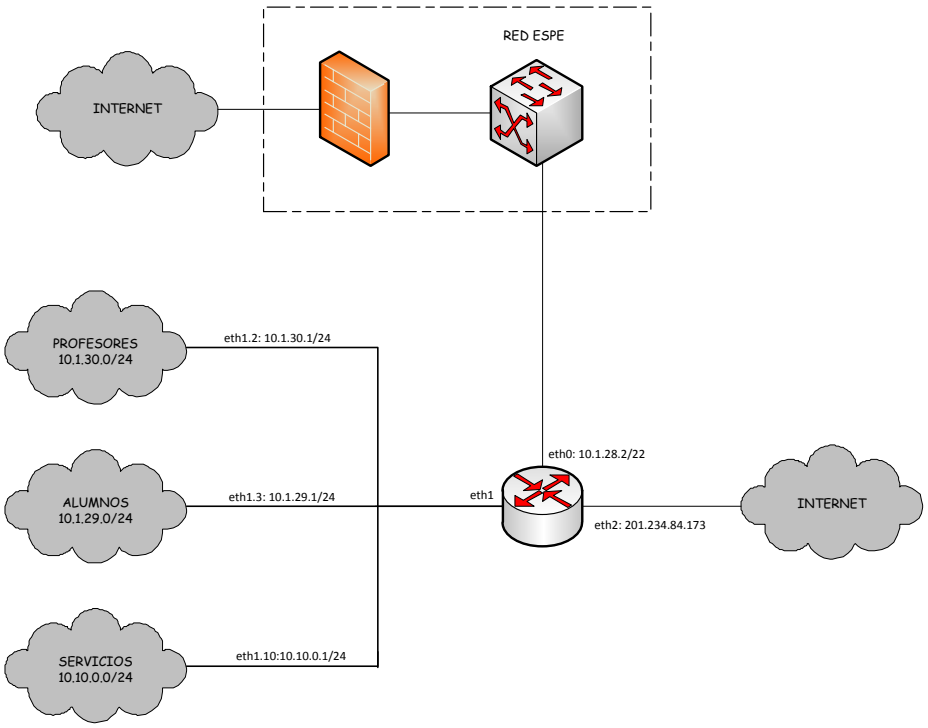


Figura. 2.13 Topología Lógica del DEEE

La manera en que los diferentes equipos se comunican dentro de la red es mediante VLANS. La configuración de VLANS está dada de la siguiente manera.

Tabla. 2.19 Información Vlans por cada Switch

VLAN ID	NAME	IP ADDRESS
1	adminEspe	
2	Masters	10.1.30.0/24
3	Pupils	10.1.29.0/24
4	Redes	
10	Intranet	10.10.0.0/24
11	Atigua	
50	NBX	
100	OUTNET	

En el Anexo A se puede observar de manera detallada como se encuentran configurados cada uno de los puertos de los Switch que conforman la red.

2.2 Análisis de los Requerimientos de Red.

2.2.1 Seguridad que emplea la red

El Departamento de Eléctrica y Electrónica emplea un mecanismo de prevención para la seguridad de la red que permiten el control de acceso y la autenticación. Los mecanismos que se encuentran implementados en la red son:

- Vlans.- Las VLANs mejoran el rendimiento de la red y aumentan la seguridad, separando sistemas que tienen datos sensibles del resto de la red.

- Firewall.- Establece un enlace controlado, protege la red local de ataques generados en el Internet proporcionando un solo punto de protección. Todo el tráfico ya se proveniente de la red o desde afuera de esta debe pasar por el firewall. Además se permitirá el envío del tráfico autorizado (definido por una política de seguridad local).
  - ACL: son reglas que, según se requiera, permiten filtrar tráfico, permitiendo o denegando el tráfico de la red.

- Servidor de Backup:

Actualmente en la red del DEEE no se utilizan ninguna herramienta ni mecanismo que nos permita detectar ataques en la red.

2.2.2 Recursos de hardware y Software empleados

Conjuntamente con las medidas de Control de Datos que proporciona el Honeywall, todo el tráfico de red que genera la Honeynet, pasará a través de un dispositivo (Switch) que podrá ser apagado por el administrador de red en caso de emergencia.

Es importante aclarar que a los Honeypots no van a tener acceso desde la red externa (internet) ya que únicamente se trata de analizar el tráfico interno, tratando de mitigar si existe potencial peligro desde los usuarios de la red.

La IP que tendrá la Honeynet fue entregada por el administrador de red del DEEE, es la 10.1.28.10 que pertenece a la red del DEEE (10.1.28.0/22). El puerto del switch al que se conecta la Honeynet, debe tener habilitados los principales puertos TCP, UDP, inclusive algunos no tradicionales y que son usado para ataques, con el fin de maximizar la efectividad de los datos recolectados y la interacción con los atacantes.

- **Requisitos de Hardware**

Para la implementación de una solución óptima se requiere los siguientes dispositivos de hardware:

- Switch: Capa 3, que permita configuración de los puertos port mirroring.
- Servidor: Disco duro de 120 GB, dos tarjetas de red PCI 10/100

- **Hardware disponible**

Se dispone de los siguientes equipos:

- Switch: El switch 10/100 Ethernet apilable 3Com® Switch 4500 26-Port ofrece switching de Capa 2 y routing dinámico de Capa 3
- Servidor: Intel Core 2 Quad, 2.4 Ghz, 2G de RAM
- 1 Tarjetas de red PCI 10/100

- **Requerimientos de Software**

El sistema operativo que requiere el host anfitrión es :

- Sistema Operativo Linux: Centos 5.4 edición de Servidor.

El software requerido para la virtualizacon es:

- Vmware Server

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 5.4 edición de Servidor.

2.2.3 Puntos Críticos

Este apartado comprende el análisis de la importancia de los servicios que presta la red del DEEE de la universidad, así como de los equipos que solicitan mayormente y aquellas que prestan dichos servicios.

En el segmento de la red que analizamos, podemos definir servicios críticos basándonos en la necesidad de ellos para los usuarios; ellos son: DHCP, DNS, WEB, Correo. Por tanto estos son los servicios que se van a implementar en la red Honeynet, puestos que son a los que principalmente acceden los usuarios, y por ende los que más pueden ser vulnerados o se presentan más visibles para los atacantes. La criticidad de cada servicio, su importancia, cantidad de usuarios, servicios, define la importancia de cada uno.

Basándonos en las figuras 2.6 y 2.8, se puede apreciar que el protocolo HTTP es uno de los más usados, por tanto el servicio web es uno de los que más tráfico genera

dentro de la red, además del tráfico generado por el uso de internet mediante el servidor proxy 10.1.0.112.

Otro punto crítico es el servidor DNS que es una de las aplicaciones con más tráfico. Tomando en cuenta la cantidad de usuarios que gestiona cada servidor y el mayor tráfico generado, está el servidor 10.10.0.2 que es el servidor web.

Otro punto de criticidad es el servidor DHCP, dado que cualquier usuario para tener conectividad dentro de la red, y poder acceder a los diferentes servicios, requiere de asignación de direccionamiento de red, entonces el servidor DHCP es otro de los puntos críticos.

Cabe resaltar además que el servidor firewall es el que proporciona todos los servicios además de las peticiones al resto de la red por medio de su direccionamiento. Por ende los servicios que se encuentran en este servidor son esenciales, y este servidor es un punto crítico ya que de sufrir algún problema, la red dejaría de funcionar.

Teniendo en cuenta que el servidor Firewall es el más importante dentro de nuestra red, se extrae los problemas de seguridad que aparecen en los datos proporcionados por los propios administradores, además, se realiza una búsqueda online de las vulnerabilidades conocidas sobre el sistema operativo y sobre los servicios implementados en cada servidor.

En caso de fallar el servicio de DHCP y DNS, toda la red perdería el acceso a servicios de la red interna por la interacción puesto que muchos utilizan los nombres de los equipos en lugar de su dirección IP entre servicios e internet.

CAPÍTULO 3

DISEÑO DE LA HONEYNET

El análisis de los patrones de ataques en la red de la DEEE, se va a realizar mediante la implementación de una Honeynet Virtual. Vamos a diseñar una honeynet utilizando el software comercial de virtualización VMware, programa con un excelente entorno de desarrollo para tecnologías Honeynet.

En este proyecto, vamos a implementar una red Honeynet Virtual GenIII (3ra. Generación) que posea un solo Honeypot. La figura 3.1 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.

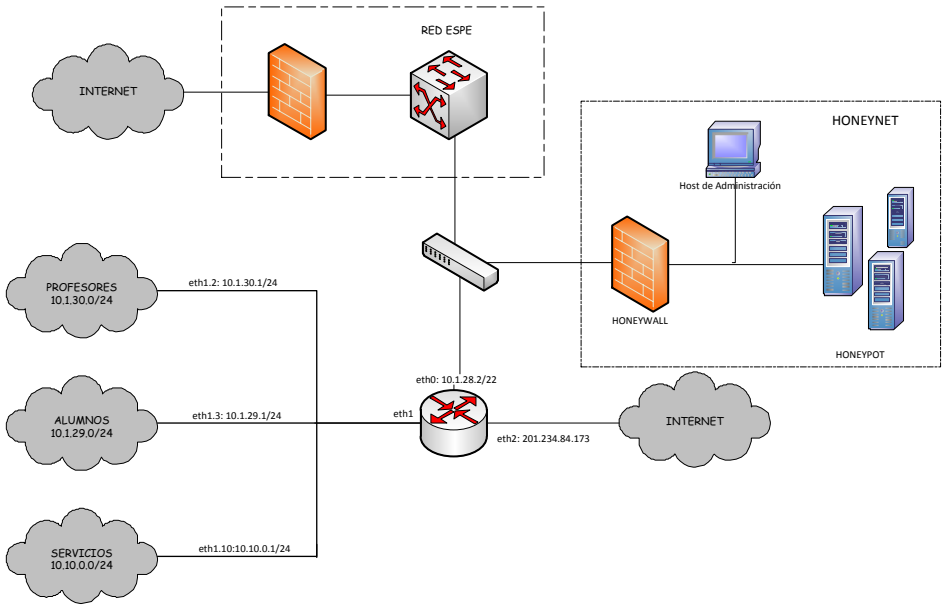


Figura. 3.1 Diseño General de la red Honeynet

3.1 Topología de red a utilizarse

Para la red Honeynet a implementarse en la red del DEEE, 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 levantaran como máquinas virtuales a todos los elementos que conforman la Honeynet.

En la Figura 3.1 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.

3.1.1 Software para Virtualización

Basándonos en lo expuesto en el capítulo 1, y luego del análisis se ha concluido utilizar a VMWARE Server, como la mejor opción para software de virtualización, gracias a que presenta importantes características, entre ellas las siguientes:

- Es la solución de virtualización más conocida y con mayor presencia comercial
- La interfaz de configuración y consola es accesible vía una interfaz Web.
- Los drivers adicionales (vmware-tools) mejoran notablemente la integración de la consola y en menor medida la performance de los discos.
- La factibilidad que proporciona para trabajar en ambientes de red, con hosts empleando diferentes modos de interfaces de red. Los modos de trabajo de las interfaces de red son: Bridge, NAT, Host-only.

3.1.2 Selección de los SO

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 5.4 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 5.4. 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.

- **Honeywall CDROM**

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.

- **Centos Server 5.4 (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 5.4 está basado en RHEL[25] 5.4 y que entre otras cosas introduce cambios importantes a la virtualización con KVM [26]y que además se ha actualizado para adaptarse al nuevo compilador, gcc 4.4.

[25] RHEL: Red Hat Enterprise Linux, Es la versión comercial basada en Fedora que a su vez está basada en el anterior Red Hat Linux
[26] KVM: Máquina virtual basada en el núcleo.

CAPITULO 4

IMPLEMENTACIÓN DE LA HONEYNET.

El host real, con SO Centos Server 5.4, se conecta directamente al switch paralelo a la red de producción. En este host procedemos a instalar el software de virtualización "VMware Server" (para más detalle de la instalación véase el Anexo B, 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

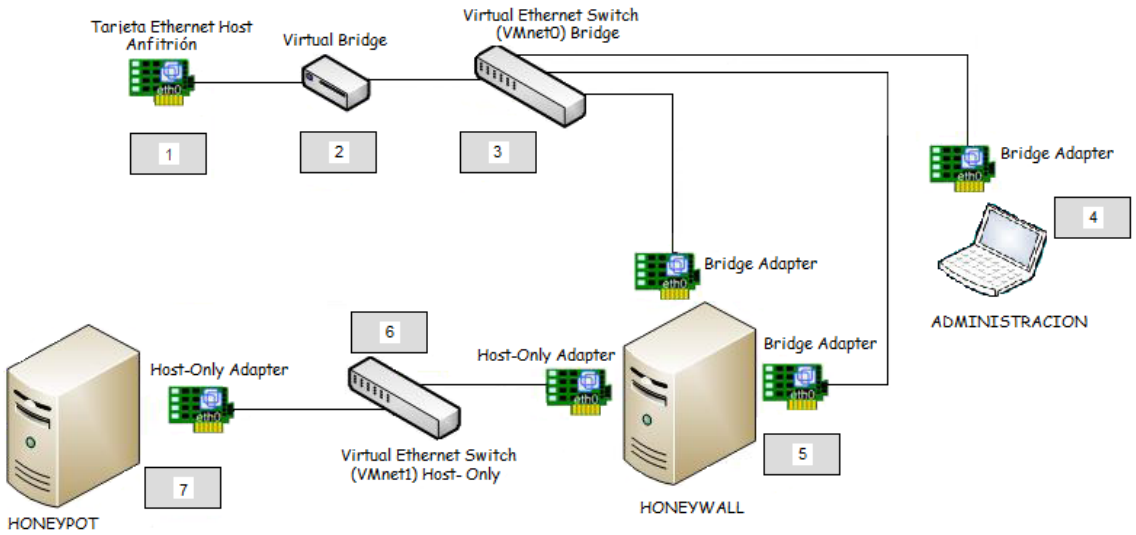


Figura. 4.1. Diagrama lógico de Honeynet virtual para el DEEE

En la Figura 4.1, 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.

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 host-only. “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 usando VMware, se configura con los requerimientos de hardware (memoria y disco) establecidos en capitulo 2, **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 usando VMware se encuentra en el Anexo C.

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. 4.1. Configuración de red de la DEEE

HONEYPOT	
IP Address	10.1.28.200
Netmask	255.255.252
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
Gateway	10.1.28.1

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

4.1.2 Instalación y configuración de los Honeypots

Se crean dos máquinas virtuales: una para el Honeypot en el cual se levantaran los servicios mencionados en el capítulo 2, 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 expuestos en el capítulo 3, 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, haciendo uso de los siguientes comandos.

- Honeypot:
  # ifconfig eth0 down
  # ifconfig eth0 10.1.28.200 255.255.252.0 10.1.28.1 10.1.31.255
  # ifconfig eth0 up

- Host de Administracion
  # ifconfig eth0 down
  # ifconfig eth0 10.1.28.254 255.255.252.0 10.1.28.1 10.1.31.255
  # ifconfig eth0 up

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, CORREO, DNS, 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 para la red de profesores.
- **DNS.-** El servidor DNS (servicio named) determina el dominio *www.deee.espe.edu.ec* para la dirección ip 10.1.28.200/22.
- **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.
- **CORREO.-** Para que el servidor de correo funcione correctamente se deben levantar los siguientes servicios: Sendmail (agente de transporte de correo),

dovecot (servidor de IMAP y POP3 de código abierto para sistemas GNU/Linux) y saslauthd (servicio de autenticación)

- **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 E.

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@localhost ~]# 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=7 ttl=64 time=0.475 ms
64 bytes from 10.1.28.200: icmp_seq=8 ttl=64 time=0.587 ms
64 bytes from 10.1.28.200: icmp_seq=9 ttl=64 time=2.86 ms
64 bytes from 10.1.28.200: icmp_seq=10 ttl=64 time=1.58 ms
64 bytes from 10.1.28.200: icmp_seq=11 ttl=64 time=0.530 ms

--- 10.1.28.200 ping statistics ---
11 packets transmitted, 5 received, 54% packet loss, time 10005ms
rtt min/avg/max/mdev = 0.475/1.208/2.865/0.925 ms
```

Figura. 4.2. Captura de Pantalla "Ping entre el Honeypot y Host de Prueba"

- 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.

  El Honeypot respondió correctamente

```
[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. 4.3. 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. Asi podemos comprobar que todos los servicios han sido iniciados y configurados correctamente:

  Accedemos desde el hots 10.1.30.132 remotamente al honeypot ……. OK

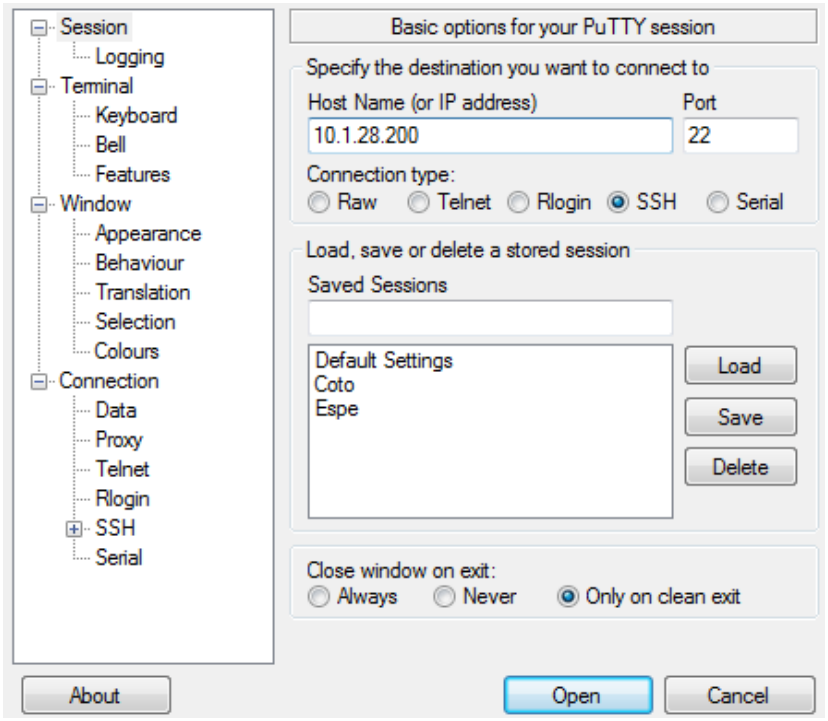


Figura. 4.4 a. Captura de Pantalla "Sesión SSH utilizando la herramienta Putty"

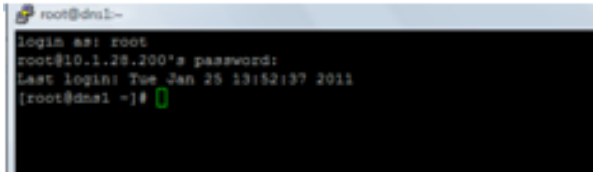


Figura. 4.4 b. Captura de Pantalla "Acceso remoto desde el Host de Prueba al Honeypot"

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

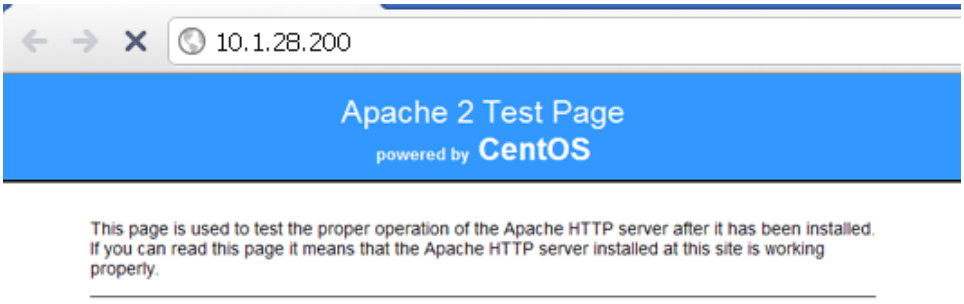


Figura. 4.5. Captura de Pantalla "Página de inicio del Servidor Web"

Accedemos desde el hots de Prueba al servicio DNS, por medio de un browser y digitando www.deee.espe.edu.int ……. OK

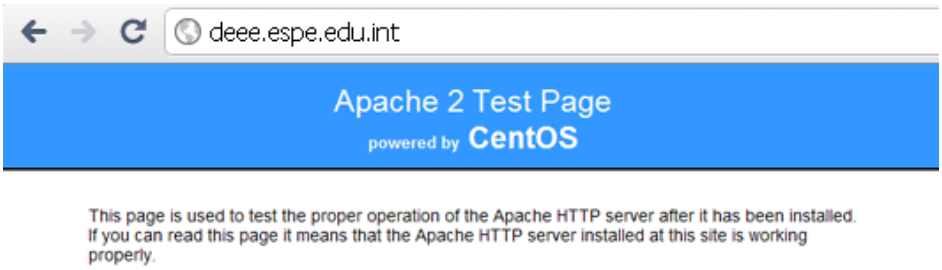


Figura. 4.6. Captura de Pantalla "Página de inicio del Servidor DNS"

En el hots 10.1.30.132, utilizando un gestor de correos, Outlook, vamos a configurar una cuenta de correo y envia mensajes de prueba, usando el servidor de correo configurado en el honeypot ……. OK

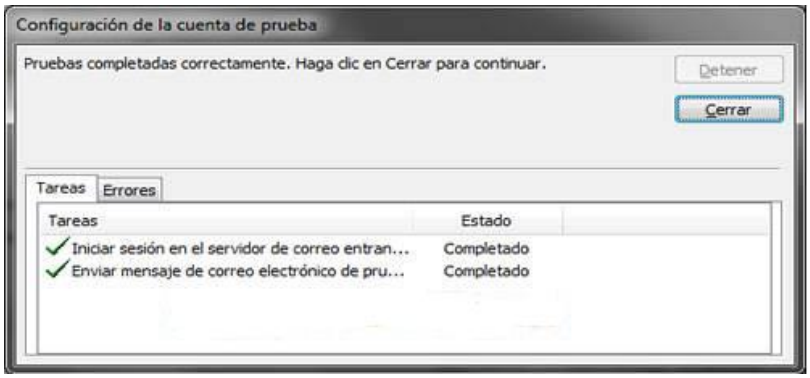


Figura. 4.7. Captura de Pantalla "Registro de usuario en el servidor de Correo"

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. ……. OK

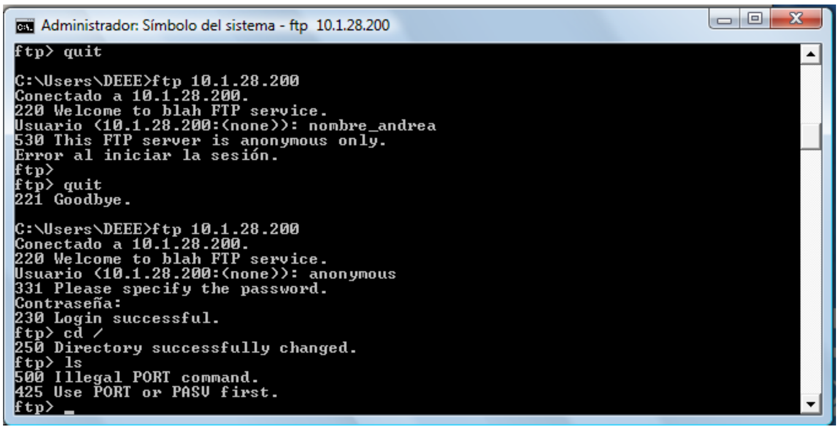


Figura. 4.8. Captura de Pantalla "Servicio FTP desde el Host de Prueba"

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

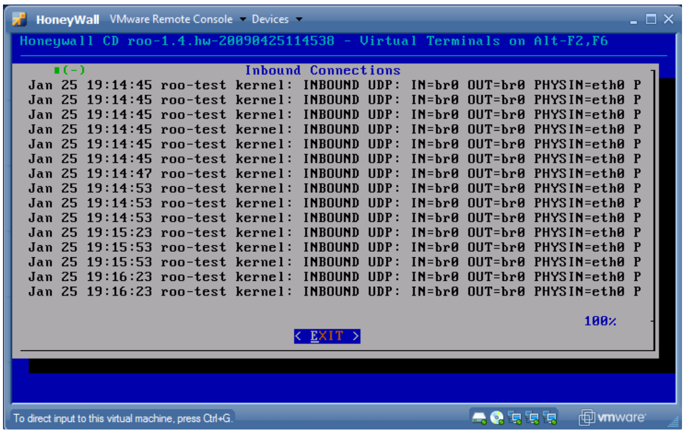


Figura. 4.9. Captura de Pantalla "Trafico entrante hacia la Honeynet"

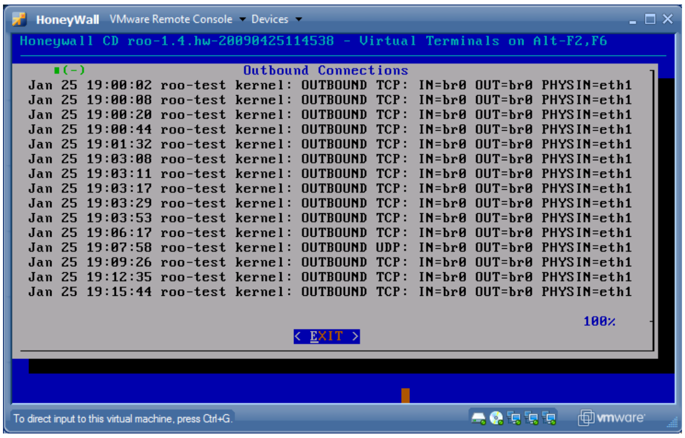


Figura. 4.10. Captura de Pantalla "Trafico saliente desde la Honeynet"

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

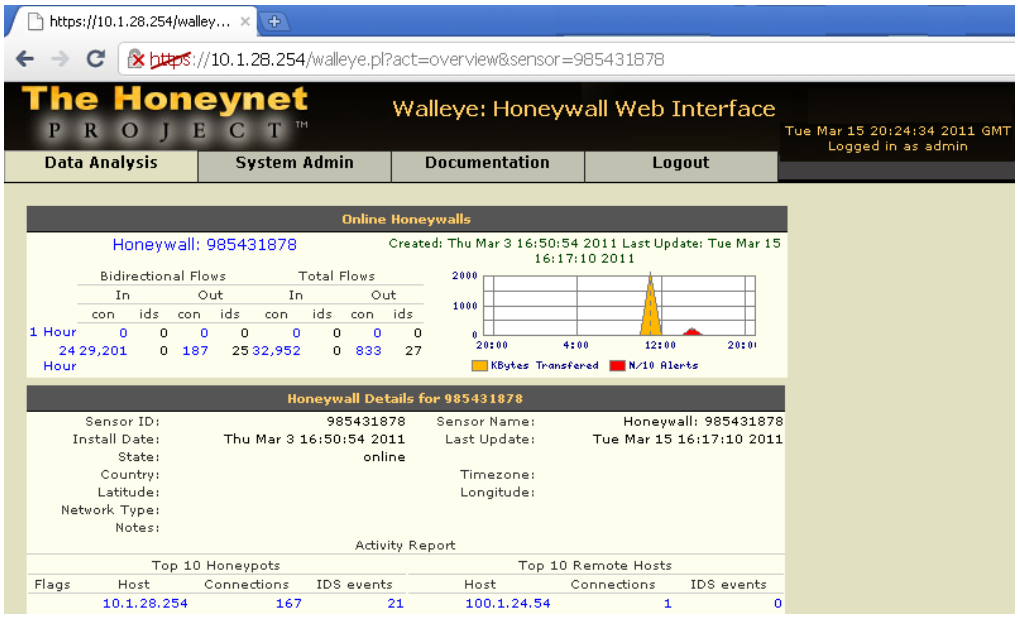


Figura. 4.11. Captura de Pantalla "Interfaz Walleye"

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 e 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 este 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 a 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.

Una cuestión importante de ahorro de tiempo (pues se debería hacer un análisis de un cierto tiempo a espera de ataques que sufra la red), y de obtener mayor conocimiento por parte del estudiante, ha motivado a desarrollar este punto.

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.- Como se explicó en el capítulo 1, 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[27] 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.[28]

  - **Ataque AMDid.-** Conjunto de herramientas para llevar a cabo ataques de DoS y MitM[29], 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.

[27] Apache.- Es un servidor web HTTP de código abierto para plataformas Unix.
[28] RAW-IP.- Protocolo
[29] MitM.- Intermediario (Men in the Middle)

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 ADMID-pack 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 asi 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

[30] PTR.- Resolución inversa. De direcciones IP a su dominio

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 [15].

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 ADMid-pkg.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

- **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

CAPITULO 5

ANÁLISIS DE TRÁFICO EN LA HONEYNET

Una intrusión consta de dos procesos, el proceso de monitorización de los eventos ocurridos en un sistema informático o una red, y el análisis de los eventos en busca de posibles intrusiones, ya sean externas como internas.

Para poder analizar los ataques se ha hecho uso de un conjunto de herramientas que permitan examinar más a fondo la cronología de los eventos, de las alertas de Snort, de los registros del Honeypot. Se puede visualizar los paquetes mediante la interfaz gráfica Walleye la cual muestra una cronología de los eventos de la Honeynet y permite almacenar toda esta información en archivos de extensión .pcap compatibles con Wireshark.

Se ha determinado una solución para incorporar las distintas herramientas instaladas en el Honeywall, al análisis para la detección de intrusiones y la activación de las alarmas.

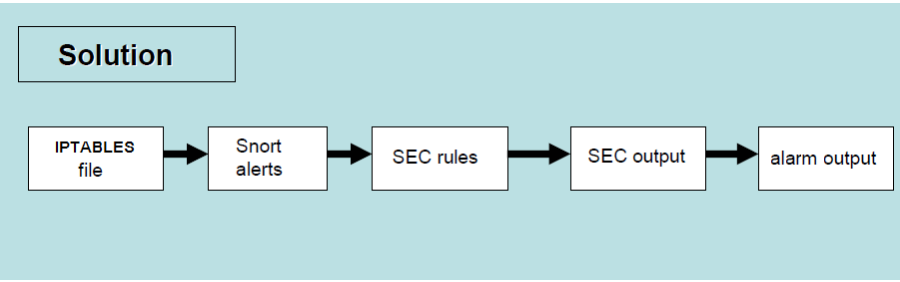


Figura. 5.1. Modo de detección de intrusiones en la Honeynet.

La Figura. 5.1 muestra el modo de operación determinado. Este modo se ha desarrollado para evitar que el sistema ignore ciertos ataques, ya sea porque el Iptables del Honeywall no registra los logs o porque el IDS Snort no detecta intrusiones, y para poder

determinar que logs pertenecen a un ataque real y cuales son parte del tráfico normal que circula por la red mediante las reglas de SEC.

El modo de operación es el siguiente. Al momento de generar el ataque, la herramienta SEC hace una correlación de los eventos ocurridos en los archivos de logs correspondientes tanto al Iptables del Honeywall como a las alertas de Snort. En consecuencia se logra que ninguna intrusión pase por alto al Honeywall, sin dejar una huella. Luego mediante la regla generada en SEC, definiendo la estructura de los logs del ataque y la cantidad de conexiones realizadas, se lleva a cabo la correlación de eventos, y se elimina los falsos positivos, dando como resultado un mensaje de alerta para cada intrusión reconocida como ataque.

5.1 Intrusiones y Detección

5.1.1 DNS ADMdnsfuckr

El IDS Snort no detecta ataques como: ADMdnsfuckr, Slowloris, debido a que requieren de la definición de reglas determinadas para cada ataque. De igual manera ocurre con el Iptables del Honeywall que no permite registrar logs de ataques como: DNSsmurf, debido a las policías empleadas en la creación de las Iptables.

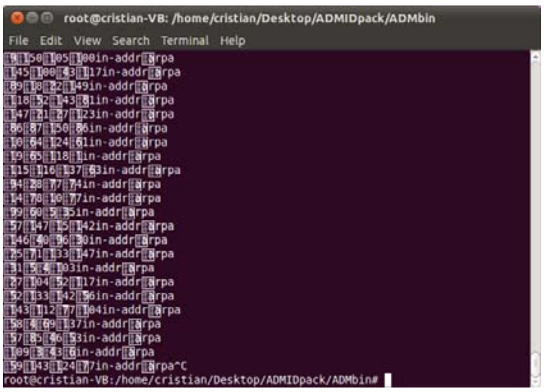
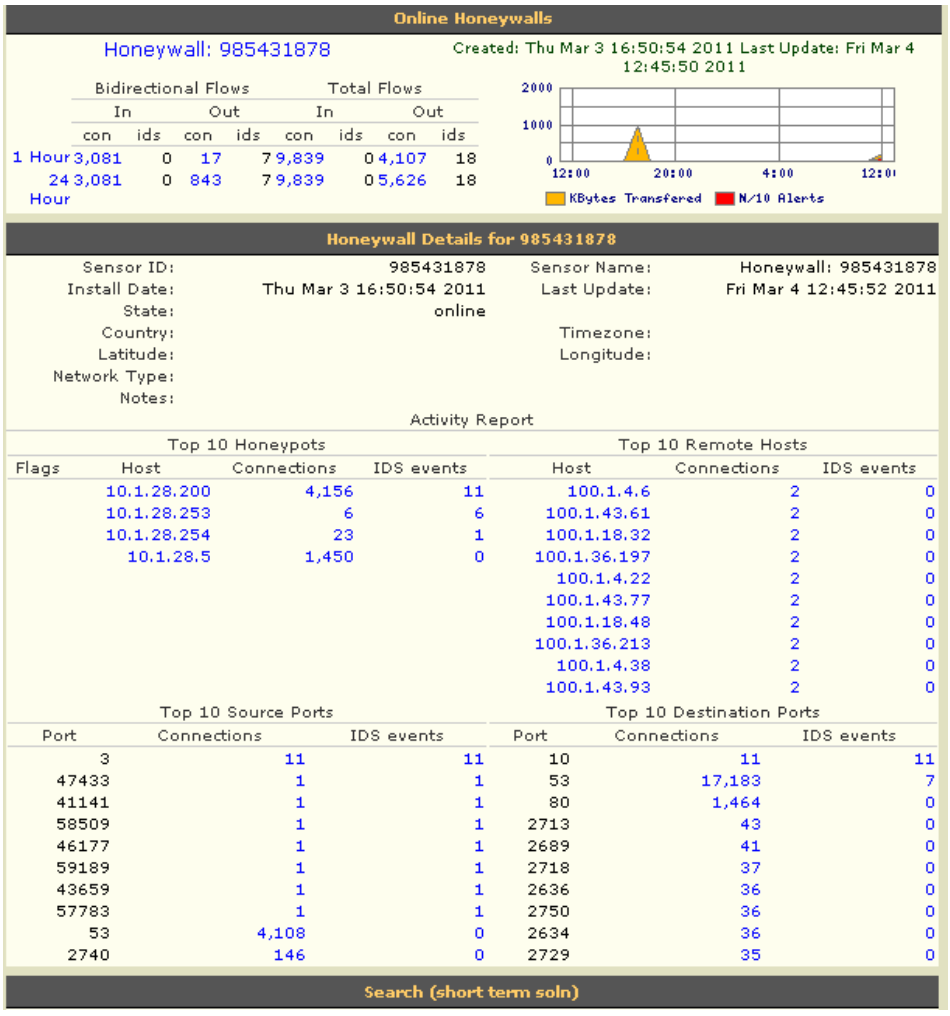


Figura. 5.2. Ejecucion Ataque DNS ADMdnsfuckr

La Figura. 5.2 muestra la ejecución del ataque al servidor DNS desde un host que pertenece a la red de profesores, en el segmento de red 10.1.30.0 y que tiene como característica enviar múltiples conexiones hacia el servidor DNS.

Una vez realizado el ataque se procede a observar que está ocurriendo en el Honeywall, se puede observar en la Figura 5.3, un incremento en el número de bytes transferidos (marca color amarillo). En el reporte de actividades se observa que aparecieron peticiones de nuevos hosts con las direcciones 100.1.x.x. Esto no es normal en el tráfico de la red, debido a que todas las peticiones deben llegar enmascaradas con la dirección 10.1.28.5. Por tanto este tráfico es extraño a la red y se procede a analizar. Aunque podemos ver que no generan ningún tipo de alerta puesto que son peticiones hechas desde diferentes hosts. Pero dado el análisis de la red efectuado en el capítulo 2, se toma en cuenta estas peticiones ya que se muestra un incremento considerable al puerto 53.



Online Honeywalls

Honeywall: 985431878 — Created: Thu Mar 3 16:50:54 2011 Last Update: Fri Mar 4 12:45:50 2011

	Bidirectional Flows				Total Flows			
	In		Out		In		Out	
	con	ids	con	ids	con	ids	con	ids
1 Hour	3,081	0	17		79,839		04,107	18
24 Hour	3,081	0	843		79,839		05,626	18

Honeywall Details for 985431878

Sensor ID:	985431878	Sensor Name:	Honeywall: 985431878
Install Date:	Thu Mar 3 16:50:54 2011	Last Update:	Fri Mar 4 12:45:52 2011
State:	online		
Country:		Timezone:	
Latitude:		Longitude:	
Network Type:			
Notes:			

Activity Report

Top 10 Honeypots

Flags	Host	Connections	IDS events
	10.1.28.200	4,156	11
	10.1.28.253	6	6
	10.1.28.254	23	1
	10.1.28.5	1,450	0

Top 10 Remote Hosts

Host	Connections	IDS events
100.1.4.6	2	0
100.1.43.61	2	0
100.1.18.32	2	0
100.1.36.197	2	0
100.1.4.22	2	0
100.1.43.77	2	0
100.1.18.48	2	0
100.1.36.213	2	0
100.1.4.38	2	0
100.1.43.93	2	0

Top 10 Source Ports

Port	Connections	IDS events
3	11	11
47433	1	1
41141	1	1
58509	1	1
46177	1	1
59189	1	1
43659	1	1
57783	1	1
53	4,108	0
2740	146	0

Top 10 Destination Ports

Port	Connections	IDS events
10	11	11
53	17,183	7
80	1,464	0
2713	43	0
2689	41	0
2718	37	0
2636	36	0
2750	36	0
2634	36	0
2729	35	0

Search (short term soln)

Figura. 5.3. Captura de Pantalla “Interfaz Wallaye: Ataque AMDdnsfuckr al servidor DNS”

En la figura 5.4 se puede observar las conexiones realizadas por los hosts 100.1.x.x, se puede observar que se generan 2 conexiones, una es la petición hacia el servidor y otra la respuesta del servidor:

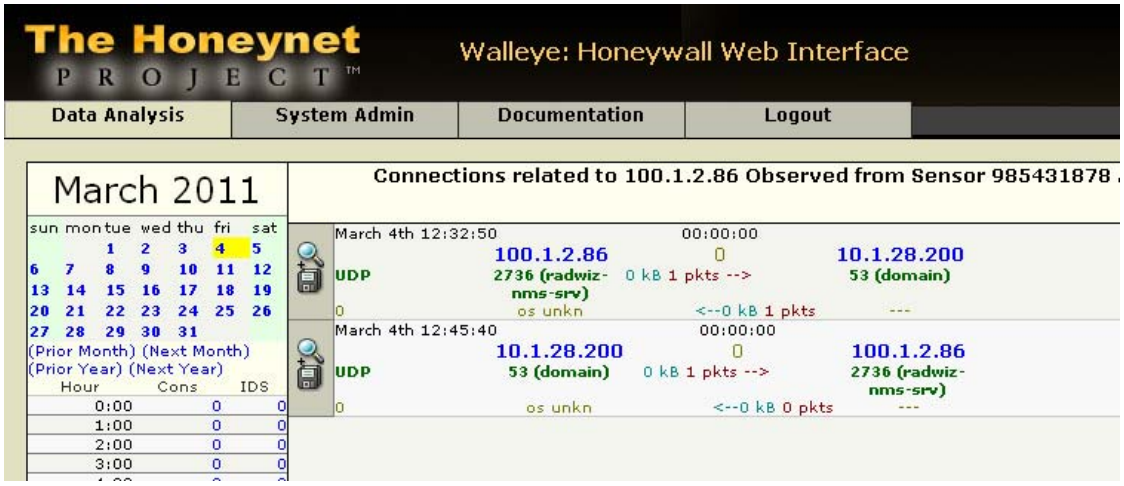


Figura. 5.4. Captura de Pantalla "Conexiones de los host 100.1.x.x al servidor DNS"

A continuación en las figuras 5.5 y 5.6 se muestran la información de los archivos de InboundConnections, es decir las conexiones entrantes hacia nuestra red, y de OutboundConections (conexiones salientes de la Honeynet) respectivamente. Estos archivos contienen información acerca de la hora, el protocolo utilizado, la cabecera del mensaje, los puertos origen/destino, las IP origen/destino, del tráfico.

```
Mar  4 12:32:50 localhost kernel: INBOUND UDP: IN=br0 OUT=br0 PHYSIN=eth0
PHYSOUT=eth1 SRC=100.1.2.83 DST=10.1.28.200 LEN=73 TOS=0x00 PREC=0x00
TTL=244 ID=49419 PROTO=UDP SPT=2601 DPT=53 LEN=53

Mar  4 12:32:50 localhost kernel: INBOUND UDP: IN=br0 OUT=br0 PHYSIN=eth0
PHYSOUT=eth1 SRC=100.1.2.84 DST=10.1.28.200 LEN=73 TOS=0x00 PREC=0x00
TTL=244 ID=1809 PROTO=UDP SPT=2628 DPT=53 LEN=53

Mar  4 12:32:50 localhost kernel: INBOUND UDP: IN=br0 OUT=br0 PHYSIN=eth0
PHYSOUT=eth1 SRC=100.1.2.85 DST=10.1.28.200 LEN=74 TOS=0x00 PREC=0x00
TTL=244 ID=51219 PROTO=UDP SPT=2733 DPT=53 LEN=54

Mar  4 12:32:50 localhost kernel: INBOUND UDP: IN=br0 OUT=br0 PHYSIN=eth0
PHYSOUT=eth1 SRC=100.1.2.86 DST=10.1.28.200 LEN=74 TOS=0x00 PREC=0x00
TTL=244 ID=16662 PROTO=UDP SPT=2736 DPT=53 LEN=54
```

Figura. 5.5. Captura de Pantalla "InboundConections de los host 100.1.x.x al servidor DNS"

```
Mar  4 12:45:40 localhost kernel: OUTBOUND UDP: IN=br0 OUT=br0 PHYSIN=eth1
PHYSOUT=eth0 SRC=10.1.28.200 DST=100.1.2.83 LEN=40 TOS=0x00 PREC=0x00
TTL=64 ID=51013 PROTO=UDP SPT=53 DPT=2601 LEN=20

Mar  4 12:45:40 localhost kernel: OUTBOUND UDP: IN=br0 OUT=br0 PHYSIN=eth1
PHYSOUT=eth0 SRC=10.1.28.200 DST=100.1.2.84 LEN=40 TOS=0x00 PREC=0x00
TTL=64 ID=16326 PROTO=UDP SPT=53 DPT=2628 LEN=20

Mar  4 12:45:40 localhost kernel: OUTBOUND UDP: IN=br0 OUT=br0 PHYSIN=eth1
PHYSOUT=eth0 SRC=10.1.28.200 DST=100.1.2.85 LEN=40 TOS=0x00 PREC=0x00
TTL=64 ID=57909 PROTO=UDP SPT=53 DPT=2733 LEN=20

Mar  4 12:45:40 localhost kernel: OUTBOUND UDP: IN=br0 OUT=br0 PHYSIN=eth1
PHYSOUT=eth0 SRC=10.1.28.200 DST=100.1.2.86 LEN=40 TOS=0x00 PREC=0x00
TTL=64 ID=29974 PROTO=UDP SPT=53 DPT=2736 LEN=20
```

Figura. 5.6. Captura de Pantalla "OutboundConections del servidor DNS al host 10.1.x.x"

En la figura 5.7 se puede observar como el servidor DNS responde a las conexiones generadas por la herramienta AMDdnsfuckr. Se puede observar que el servidor no puede resolver el nombre de dominio debido al mensaje de respuesta (networkunreachableresolving).

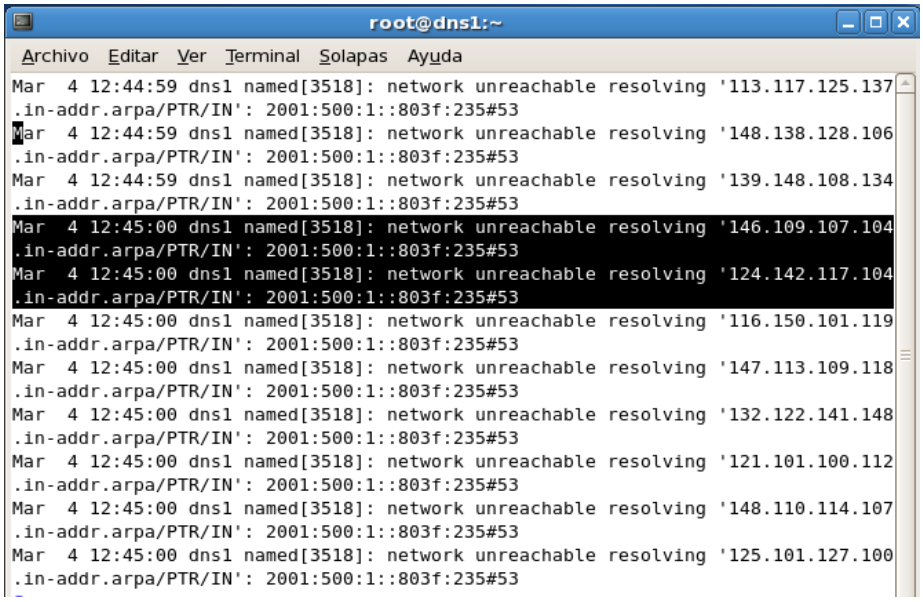


Figura. 5.7. Captura de Pantalla "Archivo de logs del Honeypot"

5.1.2 ADMkillDNS

En la figura 5.8 se puede observar cómo se lleva a cabo el ataque ADMkillDNS, que realiza una falsificación de cache del servidor de DNS.

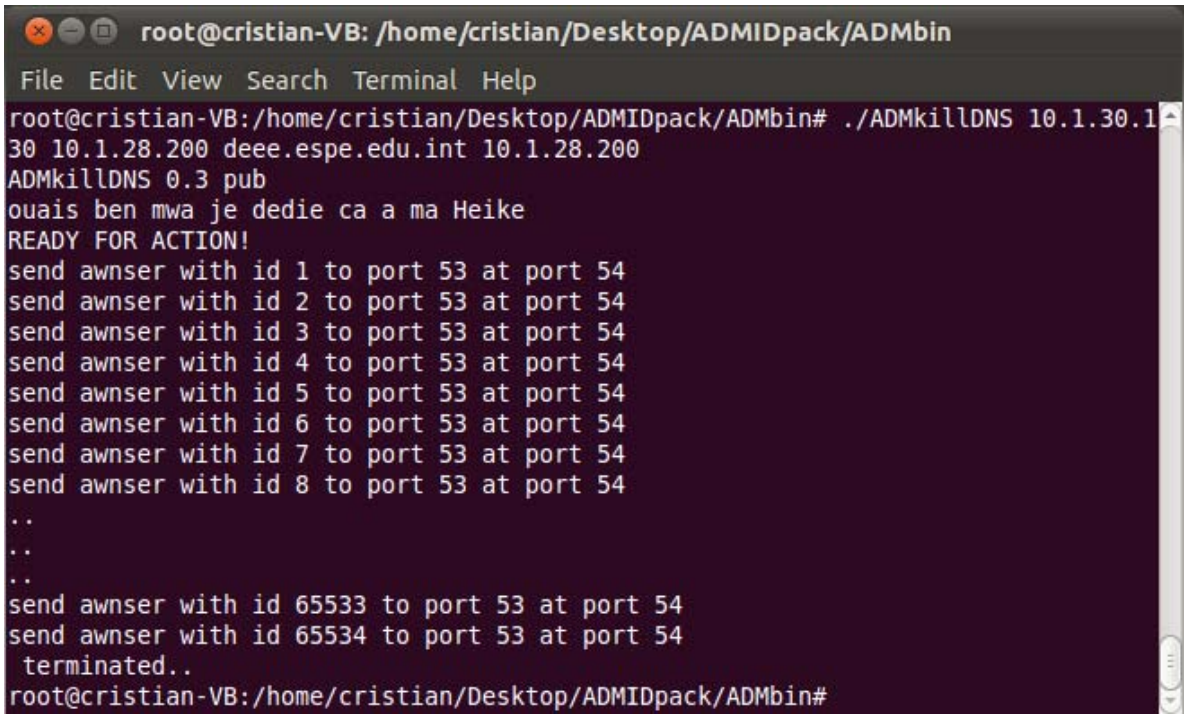


Figura. 5.8. Captura de Pantalla "Ataque ADMkilDNS"

La figura 5.9 nos muestra el ataque detectado por el IDS (Snort), el contenido de la alerta nos muestra información como:

- **03/18-20:54:29.272023** marca de tiempo.
- **1:525:9** numeración asociada a la descripción de la alerta.
- **BAD-TRAFFIC** nombre dela alerta.
- **Classification: Miscactivity** clasificación de la alerta contenida en el archivo *classification.config.*
- **Priority: 3** prioridad de la alerta.
- **UDP** protocolo asociado a la generación de la alerta.
- **10.1.28.5** origen que genera la alerta.
- **10.1.28.200** destino de quien genera la alerta.

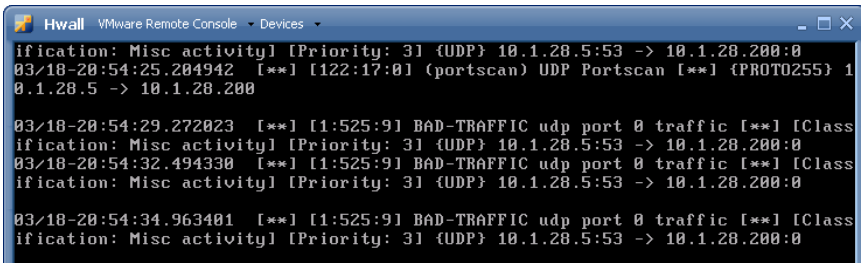


Figura. 5.9. "Alerta detectada en Snort Ataque ADMkillDNS"

En la figura 5.10 se muestra el tráfico que se detecta en el archivo **/var/log/iptables**al realizar el ataque. Como se puede observar, se realizan múltiples peticiones al puerto 53.

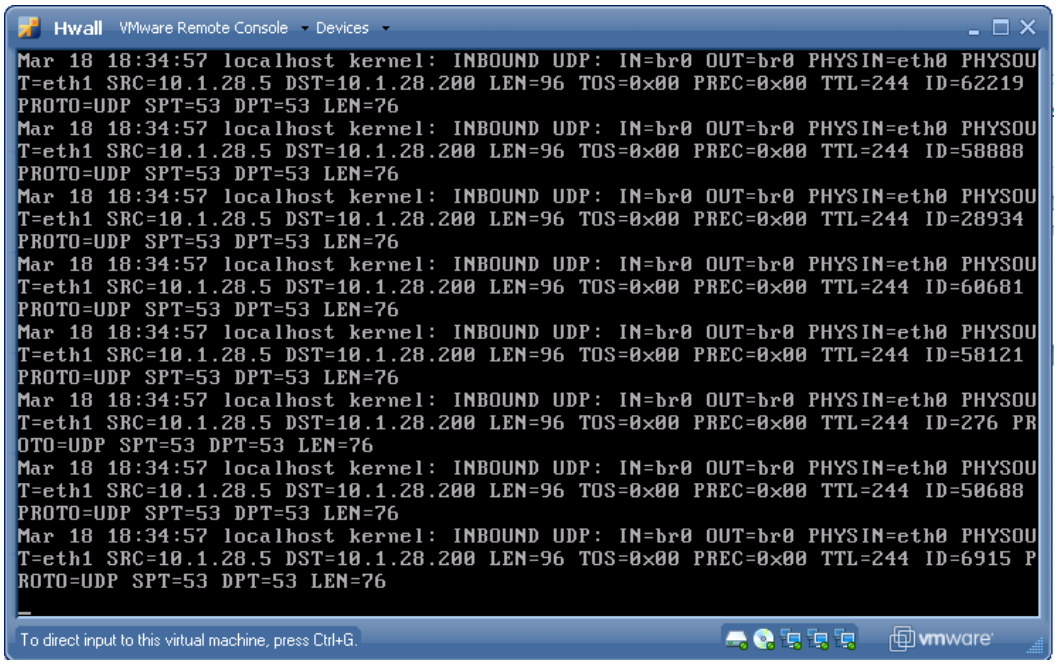


Figura 5.10. "Conexiones Detectadas en el archivo log de Iptables"

5.1.3 SLOWLORIS

La figura 5.11 muestra la ejecución del ataque de DoS hacia el servidor web, mediante el envío de múltiples conexiones.

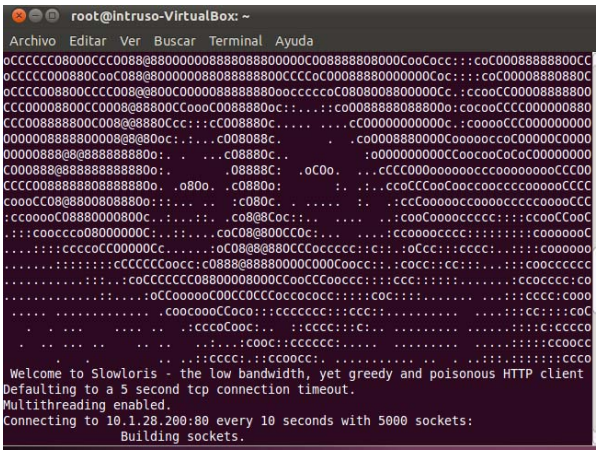
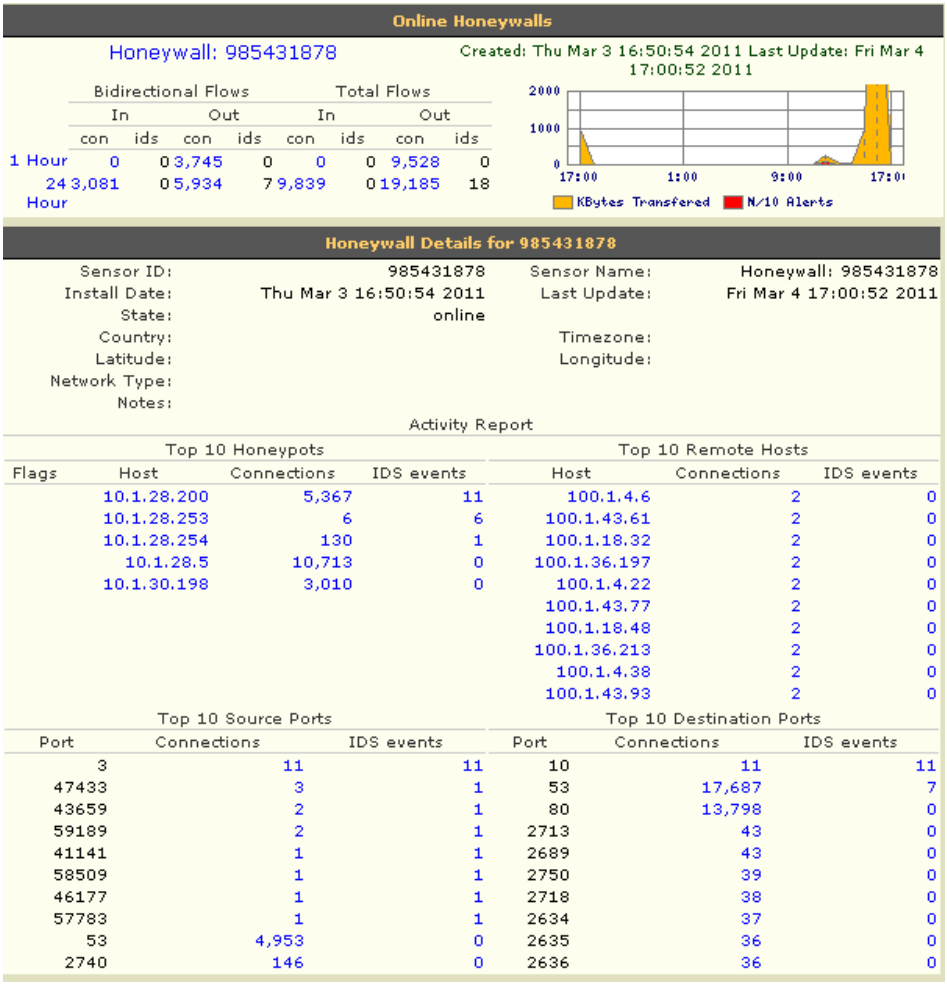


Figura. 5.11. Ejecucion del Ataque Slowloris

La figura 5.12 muestra como el Honeywall registra todas las conexiones dirigidas al Honeypot. Se puede observar que al puerto 80 se registraron 3010 conexiones desde el host 10.1.30.198.



Online Honeywalls

Honeywall: 985431878 — Created: Thu Mar 3 16:50:54 2011 Last Update: Fri Mar 4 17:00:52 2011

	Bidirectional Flows In con	ids	Out con	ids	Total Flows In con	ids	Out con	ids
1 Hour	0	0	3,745	0	0	0	9,528	0
24 Hour	3,081	0	5,934	7	9,839	0	19,185	18

Honeywall Details for 985431878

Sensor ID:	985431878	Sensor Name:	Honeywall: 985431878
Install Date:	Thu Mar 3 16:50:54 2011	Last Update:	Fri Mar 4 17:00:52 2011
State:	online		
Country:		Timezone:	
Latitude:		Longitude:	
Network Type:			
Notes:			

Activity Report

Top 10 Honeypots

Flags	Host	Connections	IDS events
	10.1.28.200	5,367	11
	10.1.28.253	6	6
	10.1.28.254	130	1
	10.1.28.5	10,713	0
	10.1.30.198	3,010	0

Top 10 Remote Hosts

Host	Connections	IDS events
100.1.4.6	2	0
100.1.43.61	2	0
100.1.18.32	2	0
100.1.36.197	2	0
100.1.4.22	2	0
100.1.43.77	2	0
100.1.18.48	2	0
100.1.36.213	2	0
100.1.4.38	2	0
100.1.43.93	2	0

Top 10 Source Ports

Port	Connections	IDS events
3	11	11
47433	3	1
43659	2	1
59189	2	1
41141	1	1
58509	1	1
46177	1	1
57783	1	1
53	4,953	0
2740	146	0

Top 10 Destination Ports

Port	Connections	IDS events
10	11	11
53	17,687	7
80	13,798	0
2713	43	0
2689	43	0
2750	39	0
2718	38	0
2634	37	0
2635	36	0
2636	36	0

Figura. 5.12. Captura de Pantalla “Interfaz Wallaye: Ataque Slowloris al servidor Web”

En la figura 5.13 se muestra las conexiones dirigidas hacia el servidor web, no existe respuesta del servidor ya que al momento que se produce este ataque el servidor inmediatamente colapsa.

Figura. 5.13. Captura de Pantalla "Peticiones del host atacante hacia el servidor Web"

Se puede observar en las figuras 5.14 y 5.15 la información de los archivos de InboundConnections y OutboundConection respectivamente. Nótese que la dirección real origen del ataque no es la del host que está realizando el ataque, esto se debe a que todas las peticiones que se realizan desde la red de la DEEE hacia el exterior salen enmascaradas con la IP: 10.1.28.5.

```
Mar  4 16:56:45 localhost kernel: INBOUND TCP: IN=br0 OUT=br0 PHYSIN=eth0
PHYSOUT=eth1 SRC=10.1.28.5 DST=10.1.28.200 LEN=60 TOS=0x00 PREC=0x00
TTL=63 ID=50056 DF PROTO=TCP SPT=44264 DPT=80 WINDOW=5840 RES=0x00
SYN URGP=0

Mar  4 16:56:45 localhost kernel: INBOUND TCP: IN=br0 OUT=br0 PHYSIN=eth0
PHYSOUT=eth1 SRC=10.1.28.5 DST=10.1.28.200 LEN=60 TOS=0x00 PREC=0x00
TTL=63 ID=39887 DF PROTO=TCP SPT=44265 DPT=80 WINDOW=5840 RES=0x00
SYN URGP=0

Mar  4 16:56:45 localhost kernel: INBOUND TCP: IN=br0 OUT=br0 PHYSIN=eth0
PHYSOUT=eth1 SRC=10.1.28.5 DST=10.1.28.200 LEN=60 TOS=0x00 PREC=0x00
TTL=63 ID=24209 DF PROTO=TCP SPT=44261 DPT=80 WINDOW=5840 RES=0x00
SYN URGP=0

Mar  4 16:56:46 localhost kernel: INBOUND TCP: IN=br0 OUT=br0 PHYSIN=eth0
PHYSOUT=eth1 SRC=10.1.28.5 DST=10.1.28.200 LEN=60 TOS=0x00 PREC=0x00
TTL=63 ID=26775 DF PROTO=TCP SPT=44262 DPT=80 WINDOW=5840 RES=0x00
SYN URGP=0
```

Figura. 5.14. Captura de Pantalla "InboundConections desde host atacante al servidor Web"

```
Mar  4 16:57:33 localhost kernel: OUTBOUND TCP: IN=br0 OUT=br0 PHYSIN=eth1
PHYSOUT=eth0 SRC=10.1.28.200 DST=10.1.28.5 LEN=546 TOS=0x00 PREC=0x00
TTL=64 ID=24394 DF PROTO=TCP SPT=80 DPT=44295 WINDOW=54 RES=0x00
ACK PSH URGP=0

Mar  4 16:57:33 localhost kernel: OUTBOUND TCP: IN=br0 OUT=br0 PHYSIN=eth1
PHYSOUT=eth0 SRC=10.1.28.200 DST=10.1.28.5 LEN=546 TOS=0x00 PREC=0x00
TTL=64 ID=43594 DF PROTO=TCP SPT=80 DPT=44296 WINDOW=54 RES=0x00
ACK PSH URGP=0

Mar  4 16:57:33 localhost kernel: OUTBOUND TCP: IN=br0 OUT=br0 PHYSIN=eth1
PHYSOUT=eth0 SRC=10.1.28.200 DST=10.1.28.5 LEN=546 TOS=0x00 PREC=0x00
TTL=64 ID=12749 DF PROTO=TCP SPT=80 DPT=44297 WINDOW=54 RES=0x00
ACK PSH URGP=0

Mar  4 16:57:33 localhost kernel: OUTBOUND TCP: IN=br0 OUT=br0 PHYSIN=eth1
PHYSOUT=eth0 SRC=10.1.28.200 DST=10.1.28.5 LEN=546 TOS=0x00 PREC=0x00
TTL=64 ID=641 DF PROTO=TCP SPT=80 DPT=44298 WINDOW=54 RES=0x00 ACK
PSH URGP=0
```

Figura. 5.15. Captura de Pantalla "OutboundConections desde el servidor Web al host atacante"

En la figura 5.16 se puede observar el archivo de logs del servidor web, como se explicó en el capítulo anterior el ataque modifica las cabeceras de las peticiones que se envían al servidor ocasionando así que el servidor web no pueda responder a ninguna petición.

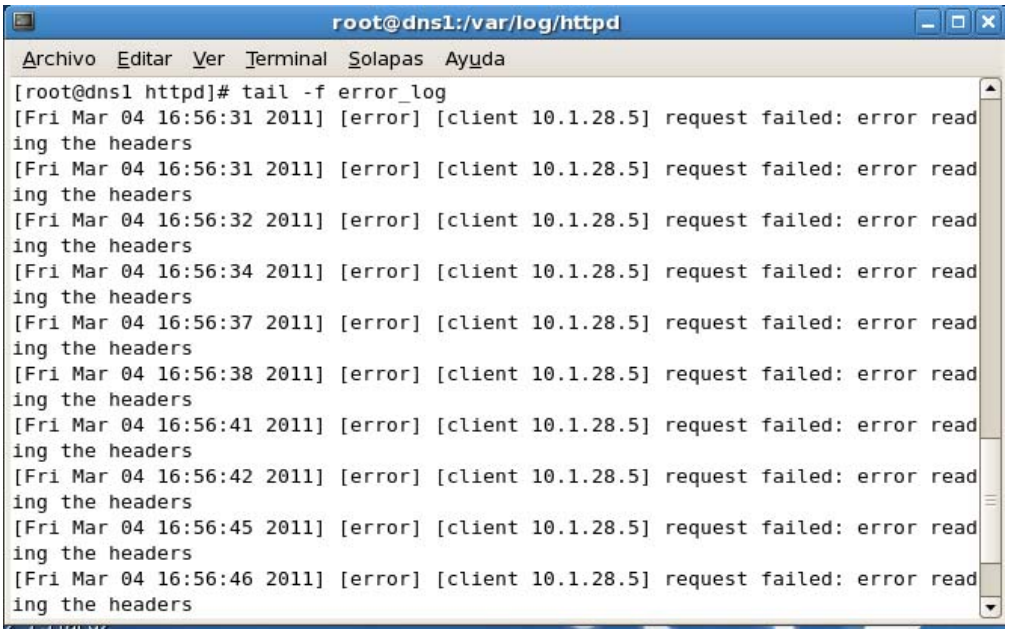


Figura. 5.16. Captura de Pantalla "Archivos de logs de error del Honeypot"

5.1.4 Hping3

En la figura 5.17 se muestra la alerta generada en Snort al realizar el ataque haciendo uso de la herramienta **hpin3,** la alerta tiene la siguiente estructura:

- **03/18-20:54:29.272023** marca de tiempo.
- **1:525:9** numeración asociada a la descripción de la alerta.
- **BAD-TRAFFIC** nombre dela alerta.
- **Classification: Miscactivity** clasificación de la alerta contenida en el archivo *classification.config.*
- **Priority: 3** prioridad de la alerta.
- **UDP** protocolo asociado a la generación de la alerta.
- **10.1.28.5** origen que genera la alerta.
- **10.1.28.200** destino de quien genera la alerta.

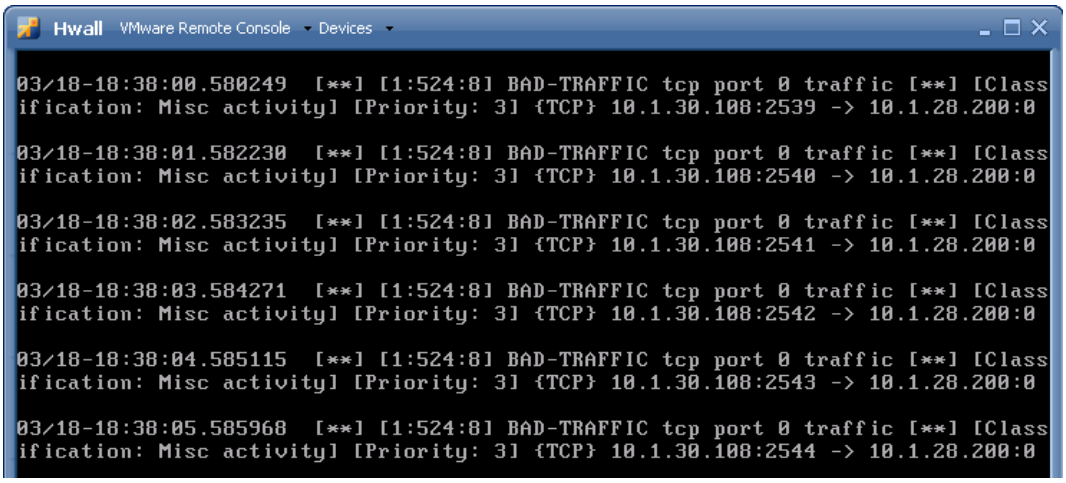


Figura. 5.17: “Alerta en Snort Ataque Hping3”

- Libpcap: apt-get install libpcap-dev (atacando desde un host Ubuntu).

- **Ataque Hping3:** Para usar **la herramienta hping3** se requiere instalar el siguiente paquete:
  - Hping3: apt-get install hping3 (atacando desde un host Ubuntu).

CAPITULO 6

PROCEDIMIENTO Y RESULTADOS

El objetivo del proyecto es detectar las vulnerabilidades y posibles ataques a los que está comprometida la red del Departamento de Eléctrica y Electrónica, es por ello que se implementó una Honeynet que es una red paralela que brinda los mismos servicios que la red del Departamento, la cual carece de seguridades ya que su objetivo es ser una red señuelo y con esto recolectar información que nos permita estudiar a fondo las técnicas utilizadas por los atacantes y saber cómo actuar ante un posible ataque a la red real.

En el capítulo 2 se realizó un análisis minucioso de tráfico de la red del departamento, el cual permite determinar los puntos críticos de la red, llegando a la conclusión que tanto el servicio de HTTP como el servicio de DNS, son los que se ven más comprometidos en la red, ya que son accedidos con mayor frecuencia por los usuarios. Por esta razón se ha decidido atacar estos servicios en la Honeynet.

6.1 Resultados obtenidos por SEC

El objetivo de SEC es correlacionar eventos, es decir, correlacionar los archivos de logs del Honeywall, permitiendo así determinar si las alertas que se generan en el IDS se tratan de un falso positivo, es decir, cuando no se trata de un ataque sino de trafico real que circula por la red.

Para hacer uso de esta herramienta es necesario analizar los archivos de logs tanto de iptables como de Snort, los cuales nos permitirán identificar patrones que se generan cuando se realiza un ataque.

Se realizaron diferentes pruebas para determinar el correcto funcionamiento de SEC en la diferenciación de falsos positivos o de un ataque. Se enviaron peticiones de usuarios a los diferentes servicios conjuntamente con los ataques obteniendo los siguientes resultados.

6.1.1 ADMdnsfucker

En la figura 6.1, se puede observar el código en SEC que permite detectar un ataque al servidor DNS. La herramienta ADMdnsfuckr envía peticiones al servidor DNS con una IP que se encuentra fuera del rango de la red del departamento, sabiendo que todas la peticiones se enmascaran con la dirección 10.1.28.5. El parámetro que permite determinar que se ha realizado un ataque es el campo SRC del log, por lo tanto definimos como patrón de búsqueda la dirección 100.x.x.x. La acción que realizara SEC es la de alertar mediante un mensaje indicando que se producido una intrusión desde la IP 100.x.x.x al puerto DNS en un hora determinada.

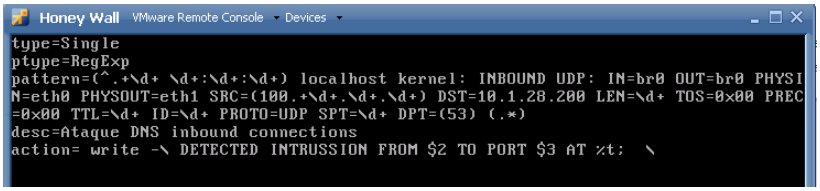


Figura. 6.1. "Codigo en SEC para detección del ataque ADMdnsfuckr"

Para la ejecución de la regla en SEC se hará uso del siguiente comando: *perl sec.pl –conf=regla.conf –input=/var/log/iptables*. En donde se indica el nombre de la regla y la entrada es decir el archivo fuente de eventos.

En la figura 6.2 se puede observar la detección del ataque, mediante la impresión de la alerta en la pantalla. Por cada log que cumpla con el patrón indicado en la regla de SEC se imprimirá una alerta.

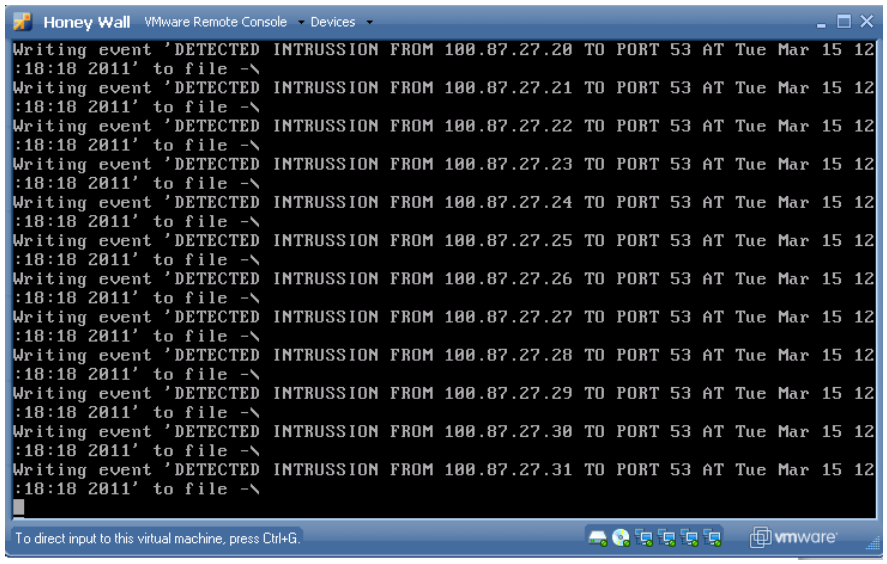


Figura. 6.2. "Alerta en SEC para el ataque ADMdnsfuckr"

6.1.2 Slowloris

En la figura 6.3 se muestra el programa desarrollado en SEC. El análisis de la red de la DEEE permite conocer el número de peticiones que diariamente se realizan al servidor Web, lo que permite definir el tipo de regla y el parámetro de condición en SEC. Luego de analizar el archivo de logs de iptables del Honeywall se determinó como parámetro un número mayor a 100 conexiones hacia el servidor web, en un intervalo de tiempo de 10 segundos. La regla SingleWithTreshold permite llevar a cabo el conteo de las peticiones al servidor Web. El segundo parámetro de condición de la regla es el puerto web (80) y el tipo de tráfico que se genera es una condición más de la regla (INBOUND TCP).

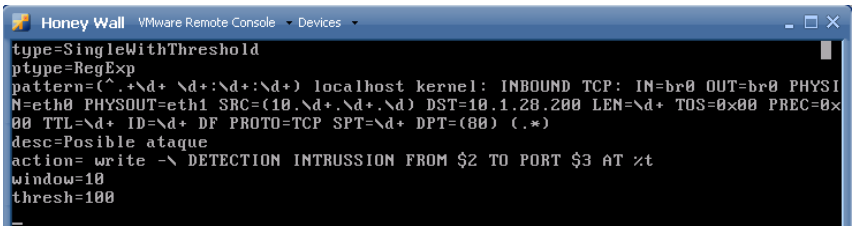


Figura. 6.3. "Programa en SEC para la detección para el ataque de Slowloris"

Para la ejecución de la regla en SEC se hara uso del siguente comando: *perl sec.pl –conf=regla.conf –input=/var/log/iptables*. En donde se indica el nombre de la regla y la entrada es decir el archivo fuente de eventos.

Se analiza el archivo /var/log/iptables donde se detecta todas las conexiones que atraviesan el Honeywall. Se aplica un filtro para definir solamente las conexiones entrantes (Inbound Connections), que tengan como destino un puerto determinado (puerto 80 para el caso del ataque http) y una dirección IP de destino definida (la dirección 10.1.28.200, IP del Honeypot que presta el servicio http).

En la figura 6.4 se observa como resultado un mensaje de alerta, indicando la hora y fecha y la dirección ip de origen de donde provienen las peticiones. El análisis de correlación mediante la herramienta SEC, según muestra la figura, permite obtener el siguiente mensaje de alerta.

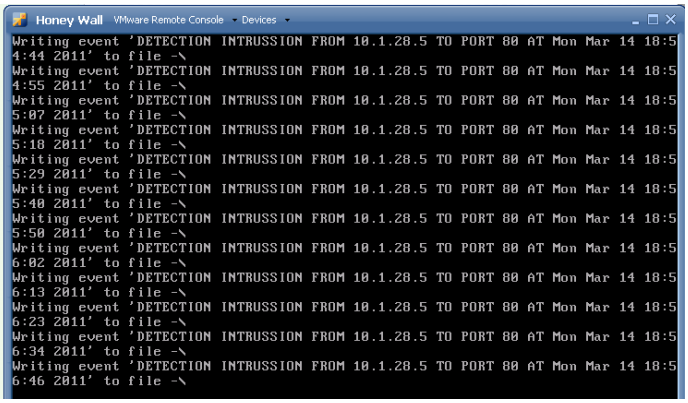


Figura. 6.4. "Alerta de SEC para el ataque de Slowloris"

6.1.3 DNS ADMkillDNS

En la figura 6.5 se puede observar el código del programa en SEC. Mediante el análisis de tráfico del Honeywall al realizar este ataque se han generado logs en el Iptables como alertas en Snort, es por ello que se ha definido dos reglas ya que se analizarán dos archivos de logs, correspondientes a cada una de las herramientas que ha detectado la intrusión. Para la primera regla se ha definido como patrón la alerta generada en Snort, usando como parámetros de condición los parámetros: BAD-

TRAFFIC (mensaje de alerta), UDP (tipo de trafico), 10.1.28.5 (IP de origen), 10.128.200 (IP destino). En la segunda regla se ha definido como patrón los logs generados por el Iptables, usando como parámetros de condición el número de peticiones hacia el puerto 53. El análisis del Honeywall permite definir 100000 peticiones hacia este servicio en un intervalo de 30 segundos.

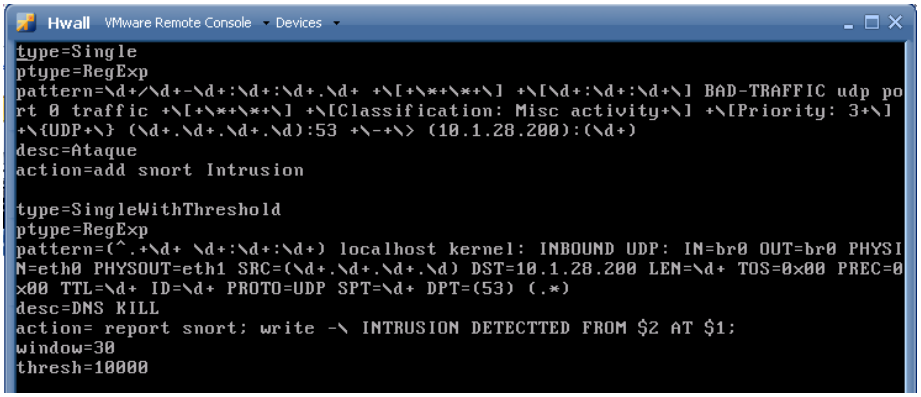


Figura. 6.5. "Código en SEC para la detección del ataque ADMkillDNS"

Para la ejecución de la regla en SEC se hara uso del siguente comando: *perl sec.pl –conf=regla.conf –input=/var/log/iptables –input=/var/log/Snort/alert*. En donde se indica el nombre de la regla y la entrada es decir los archivos fuentes de eventos.

En la figura 6.6 se muestra la alerta entregada por SEC. Se puede observar la ejecución de la acción determinada en la primera regla creando un contexto el cual lleva el mensaje de Intrusión en Snort. A continuación se ejecuta la acción correspondiente a la segunda regla en el que se imprime un mensaje confirmando la detección de la alerta en Iptables mas el contexto generado en la primera regla. Es necesario que las dos reglas se cumplan para que el ataque sea definido como tal y para que la alerta sea generada, caso contrario se tratara de un falso positivo.

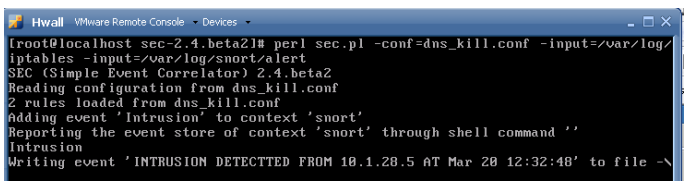


Figura 6.6. "Código en SEC para la detección del ataque ADMkillDNS"

6.1.4 Hping3

En la figura 6.7 se puede observar el código del programa en SEC. Mediante el análisis de tráfico del Honeywall al realizar este ataque se han generado una alerta en Snort, sin ser registrado el tráfico por el Iptables. La regla que se ha definido tiene como patrón la alerta generada en Snort, usando como parámetros de condición los parámetros: BAD-TRAFFIC (mensaje de alerta), TCP (tipo de trafico), 10.1.30.108 (IP de origen), 10.128.200 (IP destino).

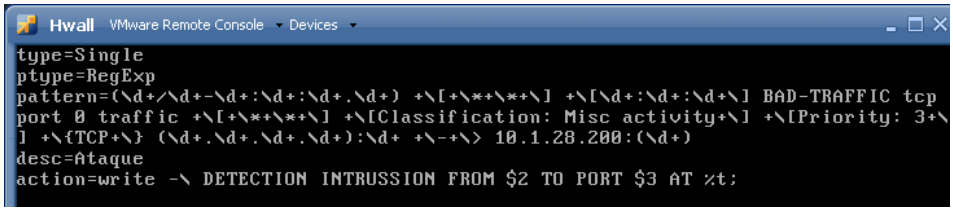


Figura. 6.7. "Código en SEC para la detección del ataque DNS Smurf"

Para la ejecución de la regla en SEC se hará uso del siguiente comando: *perl sec.pl –conf=regla.conf –input=/var/log/snort/alert*. En donde se indica el nombre de la regla y la entrada es decir el archivo fuente de eventos.

En la figura 6.8 se muestra la alerta entregada por SEC. Se puede observar la ejecución de la acción determinada en la regla indicando la IP de donde se produjo el ataque al igual que la hora y puerto al que se realizaron.

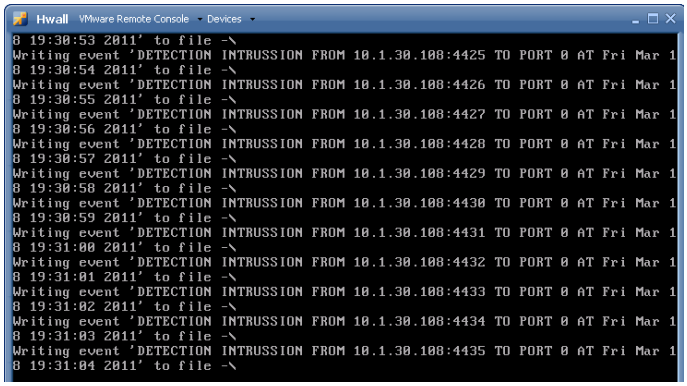


Figura. 6.8. "Alerta genera por SEC para el Ataque Hping3"

CAPITULO 7

CONCLUSIONES Y RECOMENDACIONES

7.1 Conclusiones

- El resultado de este trabajo, es el diseño e implementación de Honeynets virtuales. Para lograrlo, se ha aplicado un conjunto de herramientas de seguridad a la red. Para demostrar el funcionamiento de la Honeynet, se ha preparado un conjunto de ataques que fueron finalmente ejecutados, obteniendo resultados que nos permitieron:

    - Determinar las vulnerabilidades y puntos críticos de la red.
    - Descubrir patrones de ataques (Ej.: Ataque ADMkillDNS).
    - Recolectar toda la información acerca del atacante y su modo de operación (Ej.: Escaneo de puertos, detección de vulnerabilidades, ejecución del ataque, etc.).
    - Descubrir y manejar herramientas que permitan gestionar los eventos de seguridad ocurridos de una manera comprensible y ordenada para implementar distintos tipos de solución para cada problema encontrado.
    - Conocer cuáles son las vulnerabilidades y los ataques a los que ese encuentra expuesto el sistema y establecer a futuro políticas de seguridad que minimicen los riesgos para que alguno de estos ataques sea llevado a cabo.
    - Para lograr detectar todos los ataques que se producen en la red no es suficiente hacer uso de una solo herramienta, como se pudo ver en la

experimentación, por ellos es importante recolectar y gestionar la información de todas las herramientas en forma conjunta.

- 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.

- La implementación busca mejorar la Seguridad dentro de la red del Departamento, ya que al realizar el análisis de la red se encontró que el mismo carece de seguridades y no posee ninguna herramienta de detección de intrusiones y análisis de tráfico que permita monitorear el comportamiento de la red.

- La Honeynet por virtualización entrega una solución rentable económicamente, permite movilidad y ahorro de espacio y hardware, además de un alto rendimiento, utilizando un software de virtualización estable como VMware Server.

- En la implementación de la Honeynet, los Honeypots usarán sus servicios como recursos de red. No se ha empleado herramientas de capturas que simulen servicios de red y emulen vulnerabilidades en los servicios de red. Puede que esto aumente el riesgo de un Honeypot a ser comprometido para ser utilizado en ataques, pero nos da un ambiente de detección que permite mayor interacción con el atacante, para saber cuál es el fin del ataque y manejar las vulnerabilidades según el comportamiento de la red.

- El proyecto Honeynet utiliza de manera estándar un correlacionador de eventos llamado Sebek, en el proyecto se optó por utilizar una nueva herramienta llamada SEC que se programa en lenguaje perl para realizar la correlación de eventos. SEC nos permitió obtener resultados satisfactorios ya que detecto ataques ignorados por el IDS además de desechar falsos positivos, detectados por el IDS.

- El lenguaje perl no es de uso común para la gente qu se esta formando. Por tanto se recomienda que se imparta cusos de phyton.

- La importancia del análisis de la red en el desarrollo del proyecto nos permito 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 nos ayudó a generar las reglas de detección y analizar varia el tráfico en la red el momento de generar un ataque.

- Snort utiliza patrones para poder detectar intrusiones, es decir, detecta ataques por firmas (cabeceras de paquetes de datos definidas). Sec, por otra parte, es un correlacionador basado en eventos más no en paquetes y firmas. Esto permite que SEC detecte ataques que Snort no los detecta, debido a que cada ataque requiere una firma específica para ser detectado por Snort.

7.2 Recomendaciones

- Para que la Honeynet tengo un mejor rendimiento, se recomienda hacer uso de la gran variedad de herramientas que se pueden instalar y emplear en el Honeywall. Entre las herramientas que no se emplearon en el proyecto y se recomientda 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, etc.

- Se recomienda que en toda infraestructura de red, se integre un sistema de red paralelo, que permita detectar vulnerabilidades e información acerca de los atacantes. Por ende se recomienda que el proyecto Honeynet se extienda a todo la red del campus de la ESPE.

- Se recomienda 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.

- En el presente proyecto se ha actualizado las reglas de detección del Snort, sin embargo se recomienda instalar la última versión Snort y utilizar reglas y actualizaciones para esta versión con el fin de detectar los últimos ataques desarrollados.

- 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.

- Según las aplicaciones y tráfico que maneje la red a la cual se desea implementar el Proyecto Honeynet se debe considerar que existen honeypots ya desarrollados que nos permiten emular equipos de detección con diferentes características, uno de ellos es Honeyd que puede emular miles de diferentes tipos de ordenadores en el mismo tiempo. Teniendo al alcance honeypots ya desarrollados con diferentes características dependiendo del tipo de intrusos que queremos detectar, ya sea según ataques a servicios, a puertos o a aplicaciones, podemos considerarlos e implementarlos.

- Se ha desarrollado ataques de Fuerza Bruta. Se ha escogido implementar este tipo de ataques debido a que presentan comportamientos repetitivos y permiten detectar las intrusiones por las múltiples conexiones realizadas como condición para el patrón de conexión. Ahora para analizar ataques de otro tipo no vamos a poder utilizar este análisis. Se recomienda realizar pruebas para otros tipos de ataques, no solo de Fuerza Bruta.

REFERENCIAS BIBLIOGRAFICAS

- [1] http://pi1.informatik.unimannheim.de/filepool/publications/vulnerabilityassessment-using-honepots.pdf, ***"Vulnerability Assessment using Honeypots"***.
- [2] http://www.sisteseg.com/files/Microsoft_Word_SEMINARIO_SEGURIDAD_DE_REDES_web.pdf, ***"Seminario Seguridad en Redes"***
- [3] http://his.sourceforge.net/honeynet/papers/honeynet/, ***"Proyecto Honeynet"***
- [4] http://jungla.dit.upm.es/~jlopez/publicaciones/mundointernet04.pdf, ***"Honeynets"***
- [5]http://www.honeynet.unam.mx/docs/Intro.pdf, ***"Introduccion a las Honeynets"***
- [6]Fernández Hugo Héctor: ", Universidad Nacional Del Comahue, Neuquén, Argentina, disponible en: http://www.fing.edu.uy/inco/eventos/cibsi09/docs/Papers/CIBSI-Dia2-Sesion4(5).
- [7]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, Guayaquil Ecuador, disponible en: www.dspace.**espol**.edu.ec/handle/123456789/4203?mode=full
- **[8]** http://linux.die.net/man/1/sec, ***"Working with SEC"***
- **[10]**http://geeks.ms/blogs/jalarcon/archive/2009/10/25/virtualbox-virtualizaci-243-n-de-alto-rendimiento-y-gratuita.aspx, ***"VirtualBox Virutualizacion de Alto Rendimiento"***
- **[11]**http://www.elartedeprogramar.cl/linux_so/introduccion_virtualizacion_xen_191.0.html , ***"Introducción a la Virtualización Xen"***
- **[9]**http://tuquiosco.es/virtualizacion/productos-virtualizacion-vmware/, ***"Pruductos de Virtualización VMware"***
- **[12]**http://www.alegsa.com.ar/Dic/vulnerabilidad.php, ***"Vulnerabilidades"***
- **[13]** Acosta, Nicolás., Buitrago, Ricardo., Newball, Mc'Carthy., Ramírez, Maria A. y Sánchez, Julián. **"Análisis de Vulnerabilidades"**, Universidad de los Andes. Disponible en:

http://www.criptored.upm.es/guiateoria/gt_m142o.htm

- **[14]** http://www.scribd.com/doc/36013250/Tipos-de-Ataques-e-Intrusos-en-Las, ***"Tipos de Ataques e Intrusos en las Redes"***
- **[15]** http://tecnoquia.blogspot.com/2009/12/port-mirroring-en-switches-3com.html**,** ***"Port Mirring en Switches 3Com"***
- http://www.mike.com.mx/UAT_Honeypots.pdf, ***"Honeypots"***
- http://www.tic.udc.es/~nino/blog/psi/2010/ataque-dns.pdf, ***"Ataque DNS"***
- **[16]**http://searchenterpriselinux.techtarget.com/tip/Simple-Event-Correlation-installation-and-configuration, ***"Installtion and Configuration Simple Event Correlation"***
- http://www.iberprensa.com/todolinux/articulos/TL65_42-46%20Taller_Log.pdf, ***"Trabajando con los Logs"***
- http://www.htmlpoint.com/perl/perl_11.html, ***"Expresiones regulares perl"***

ANEXO A

CONFIGURACION DE LOS SWITCHS DEL DEEE

A continuación de detalla la configuración de cada uno de los Switch que pertenecen a la red del DEEE, que Vlan está configurada en cada uno de sus puertos.

- **BLOQUE A1**

  - SWITCH1-A1 (Mayo)
    IP:10.10.0.250
    GW:10.10.0.1

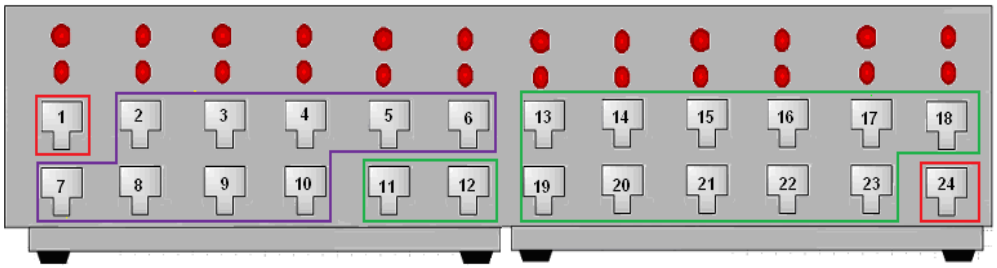


Figura. A.1. Switch 1 Rack A1 Vlans

1. –
2. A1-2313
3. A1-2314
4. A1-2315
5. A1-2316
6. A1-2317
7. A1-2318
8. A1-2319
9. A1-2320
10. A1-2324
11. Hub 3Com (Puerto 1)
12. A1-2309
13. A1-2201
14. A1-2202
15. A1-2203
16. A1-2205
17. A1-2204
18. A1-2206
19. A1-2207
20. A1-2208
21. A1-2209
22. A1-2210
23. A1-2211
24. –

VLANS

Profesores

Alumnos A1

Todas las VLANs

- **BLOQUE B1**

  - SWITCH1-B1 (Julio)

    IP:10.10.0.251

    GW:10.10.0.1

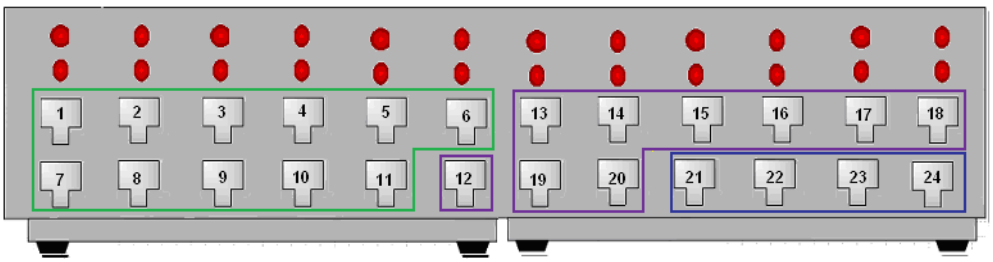


Figura. A.2. Switch 1 Rack B1 Vlans

1. B1-1301
2. B1-1302
3. B1-1303
4. B1-1304
5. B1-1305
6. –
7. B1-1306
8. B1-1307
9. B1-1308
10. B1-1205
11. Hub Uplink
12. –
13. B1-1206
14. B1-1207
15. B1-1208
16. B1-1209
17. B1-1210
18. –
19. B1-1211
20. B1-1212
21. B1-1201
22. B1-1202
23. B1-1203

24. B1-1204

VLANS
Profesores
Alumnos B1
TRK al B2

- **BLOQUE B2**

  - SWITCH2-B2 (Enero)

    IP:10.10.0.254

    GW:10.10.0.1

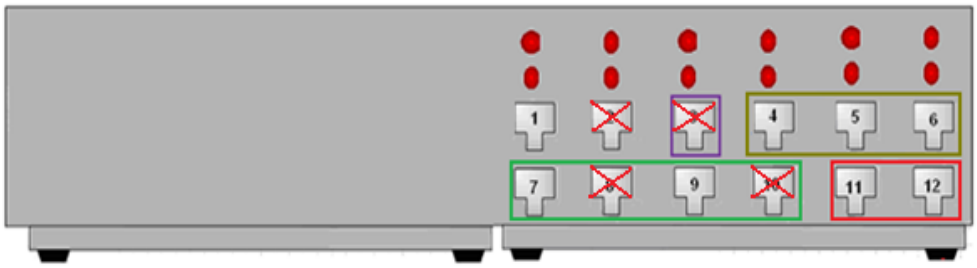


Figura. A.3. Switch 2 Rack B2 Vlans

1. Switch 3Com (Puerto 12)
2.-
3.-
4. B2-0222
5. –
6. RAS
7. Hub3-B2 (Puerto 16)
8. –
9. Hub2-B2 (Puerto 16)
10. -
11. B2-0201
12. B2-0220

VLANS
Profesores
Intranet
Alumnos B2
Todas las VLANs

  - SWITCH3-B2 (Febrero)

IP:10.10.0.253
GW:10.10.0.1

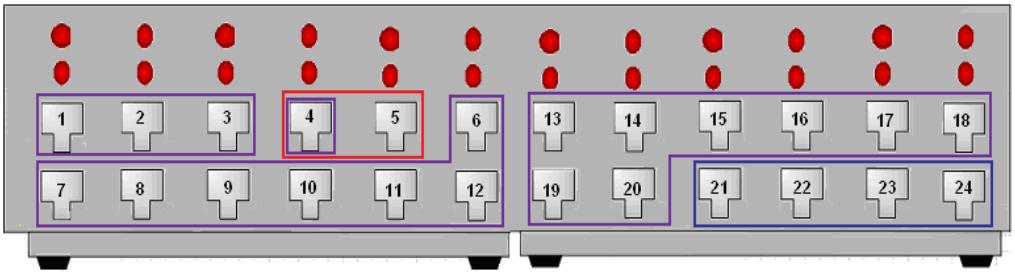


Figura A.4 Switch 3 Rack B2 Vlans

1. B2-0401
2. B2-0402
3. B2-0403
4. B2-0404
5. B2-0405
6. B2-0406
7. B2-0407
8. B2-0408
9. B2-0409
10. B2-0410
11. B2-0411
12. B2-0412
13. B2-0419
14. B2-0418
15. B2-0421
16. B2-0422
17. B2-0423
18. B2-0424
19. B2-0321
20. B2-0322
21. B2-0205
22. B2-0206
23. B2-0207
24. B2-0208

VLANS
Profesores
TRK al B1
Todas las VLANs

- SWITCH4-B2

  IP:10.10.0.247

GW:10.10.0.1

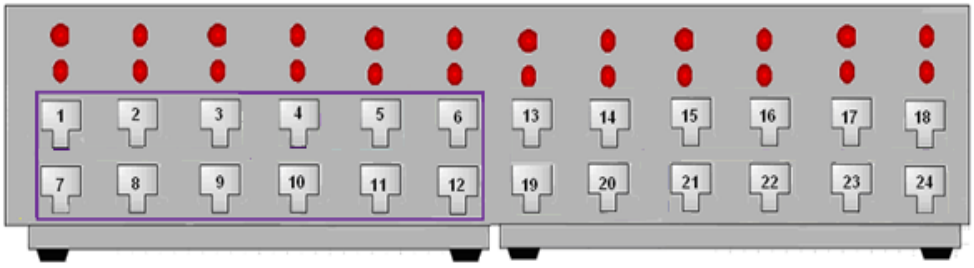


Figura. A.5. Switch 4 Rack B2 Vlans

- SWITCH5-B2

  IP:10.10.0.253

  GW:10.10.0.1

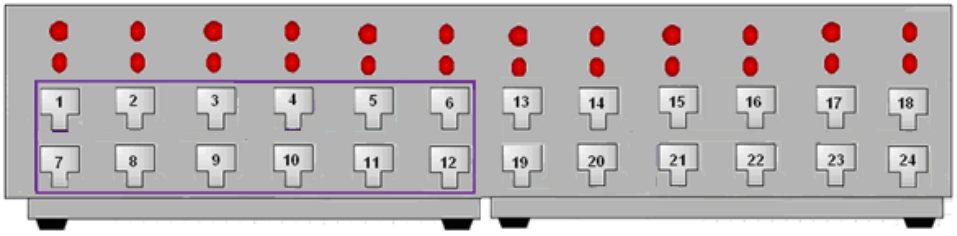


Figura. A.6. Switch 5 Rack B2 Vlans

- **BLOQUE C1**

  - SWITCH1-C1 (Junio)

    IP:10.10.0.249

    GW:10.10.0.1

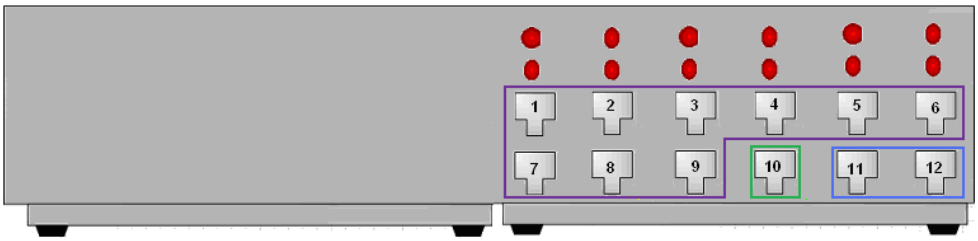
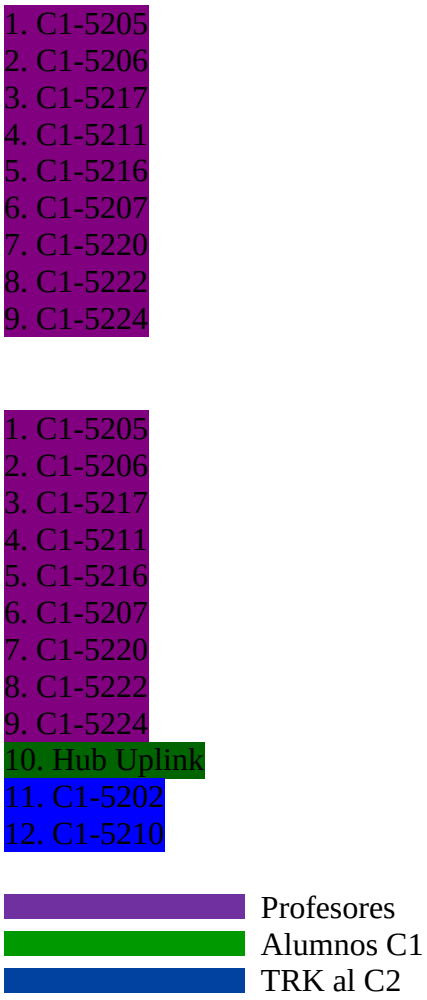


Figura. A.7. Switch 1 Rack C1 Vlans


1. C1-5205
2. C1-5206
3. C1-5217
4. C1-5211
5. C1-5216
6. C1-5207
7. C1-5220
8. C1-5222
9. C1-5224
1. C1-5205
2. C1-5206
3. C1-5217
4. C1-5211
5. C1-5216
6. C1-5207
7. C1-5220
8. C1-5222
9. C1-5224
10. Hub Uplink
11. C1-5202
12. C1-5210
Profesores
Alumnos C1
TRK al C2

ANEXO B

INSTALACIÓN Y CONFIGURACIÓN DE VMWARE

- **Instalación de paquetes requeridos**

Antes de instalar VMware Server, es necesario instalar algunos prerrequisitos:

- Librerias de desarrollo (Development Libraries)
- Herramientas de desarrollo (Development Tools)
- Paquete xinetd
- Paquete kernel-devel. Por favor, asegúrese de escoger el paquete kernel-devel que corresponda a su kernel actual

- **Instalación de Vmware**

1. Descargar VMware Server para Linux. archivo tar.gz mediante el siguiente comando: *wget http://www.vmware.com/download/server/*
2. Descomprimir el archivo VMware Server. tar.gz y ejecutar el programa de instalación: *tar xvfz VMware-server-*.tar.gz*

- **Configuración de Vmware**

1. Una vez instalado el VMWare, el siguiente paso es su configuración, donde es necesario ejecutar el comando*: vmware-config.pl*
2. Al final de la instalación, se le pedirá que introduzca un número de serie:

   Please enter your 20-character serial number.

   Type XXXXX-XXXXX-XXXXX-XXXXX or 'Enter' to cancel:

   Escriba su número de serie para VMware Server, que se lo puede obtener del sitio oficial de VMware.
3. Finalmente reinicie el servicio de Vmware

ANEXO C

CONFIGURACIÓN DE LAS MÁQUINAS VIRTUALES

1. Ingresar a la web de administración del VMware Server, mediante un browser digitamos https://xxx.xxx.xxx.xxx:8333, donde xxx.xxx.xxx.xxx es la ip del equipo remoto.

2. Una vez autenticado el usuario, se debe realizar click sobre "Create Virtual Machine" crear máquina virtual. Esto desplegará un asistente para la creación de la máquina virtual.

3. La primera definición que se debe realizar es el nombre y ubicación si se dispone de más de una (datastore -> almacenamiento de datos).

4. El siguiente paso es seleccionar el sistema operativo que ejecutará el equipo virtualizado.

5. En este paso se comienza a definir el hardware del equipo. En este caso es la memoria (este valor es fácilmente modificable más adelante) y el procesador (en algunos sistemas operativos puede generar conflictos pasar de un núcleo a varios o la inversa).

6. El siguiente paso corresponde definir el disco duro. Se puede utilizar un disco duro de una máquina virtual ya existente, crear uno o no agregar el dispositivo

7. A continuación se debe definir sobre dispositivo de red va a poseer la máquina virtual.

8. Definir los dispositivos cdrom y floppy. En ambos casos se puede vincular los dispositivos virtuales con dispositivos físicos del equipo anfitrión o utilizar imágenes.

9. El último paso es definir si se quiere utilizar dispositivos USB o no en este equipo. En la mayoría de los casos esto no es necesario.

Finalizada la configuración del equipo, se presenta una ventana con la información del mismo y brinda la posibilidad de agregar otro componente. Para iniciar la máquina virtual se debe presionar el botón verde de "Play" en la parte superior de la pantalla.

ANEXO D

INSTALACIÓN Y CONFIGURACIÓN DEL HONEYWALL ROO V1.4

- **Pasos para la instalación**

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

Figura. C.1. 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*

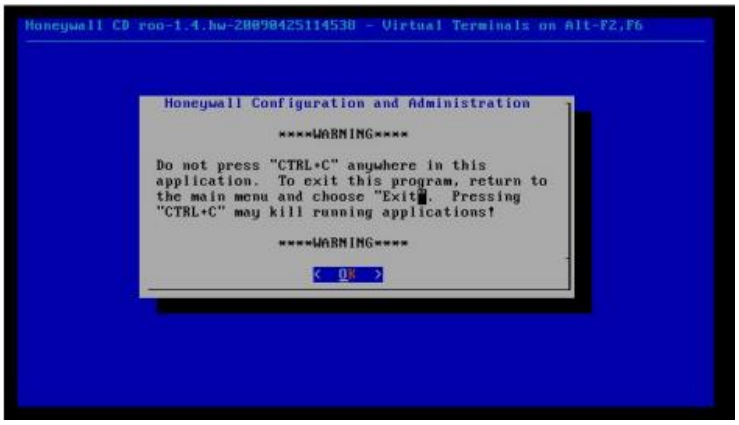


Figura. C.2. Pantalla de advertencia del Honeywall

Para proceder a configurar el Honeywall se debe Seleccionar Honeywall Configuration

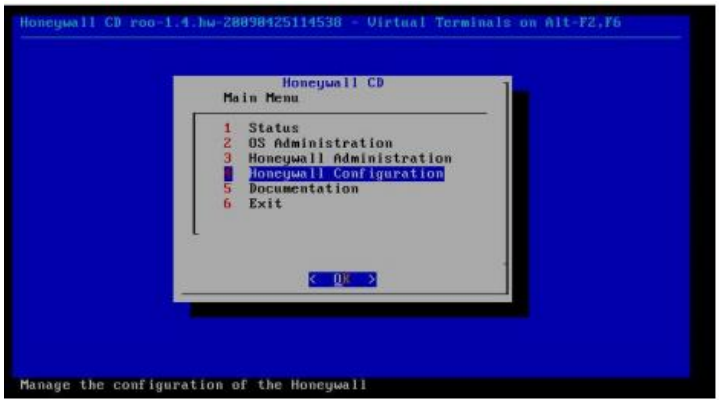


Figura. C.3. Inicio de la configuración del Honeywall

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

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

Figura. C.4. Selección del tipo de configuración

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

Figura. C.5. Ingreso de las direcciones Ips de los Honeypots

Ingrese las direcciones IP de la Honeynet

Figura. C.6. Ingreso de la dirección IP de la Honeynet

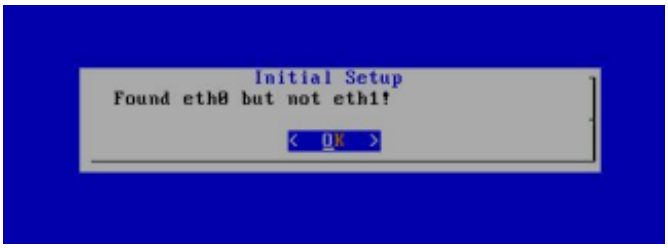


Figura. C.6. Interface eth0 y eth1 encontrada

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

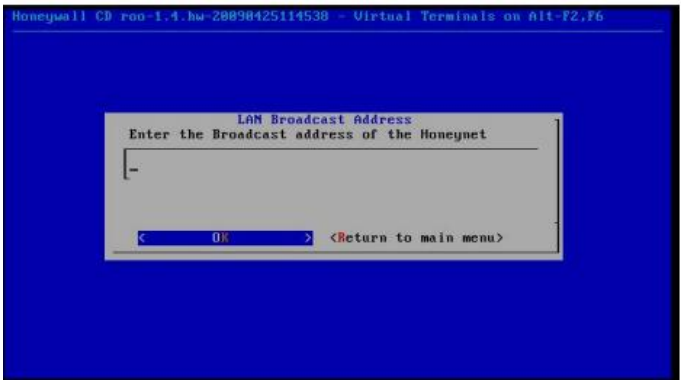


Figura C.7 Ingreso de las direcciones broadcast de la red LAN

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

Figura C.8 Inicio de la configuración de interface de administración

Configuración SSH

Figura C. 9 Inicio de la configuración de SSH

Permitir el logearse remotamente por SSHD

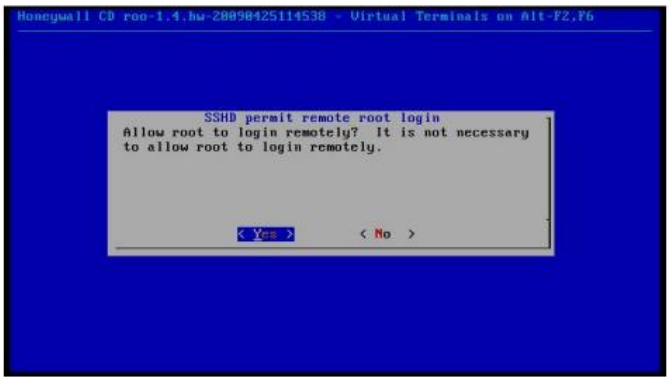


Figura C. 10 Login remotamente como root

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

Figura C. 11 Cambio de la contraseña de root

Figura C. 12 Cambio de la contraseña de roo

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

Figura C. 13 Puerto TCP permitido para acceder a la administración web del Honeywall

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

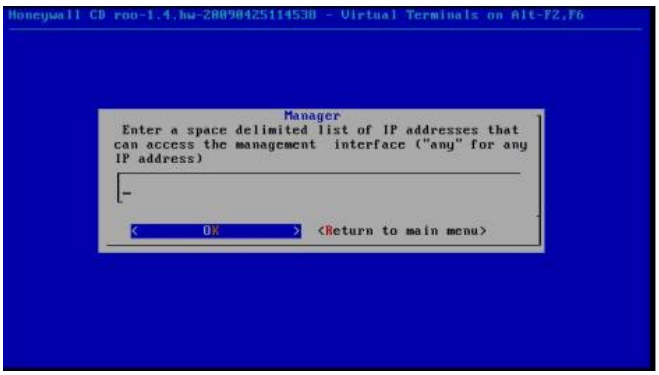


Figura C. 14 Ingreso de la IP para acceder a la web de administración

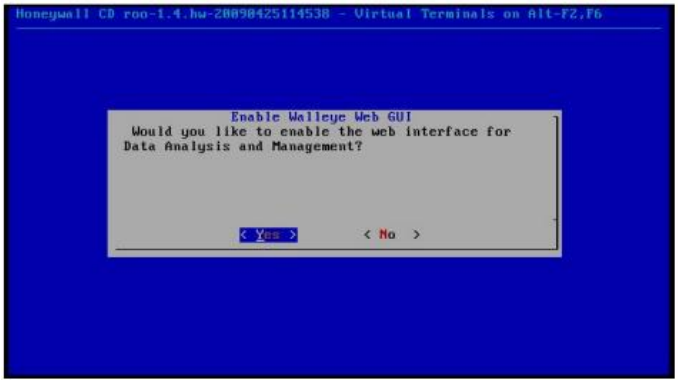


Figura C. 15 Habilitar la interfaz web de administración

Activar las restricciones del firewall para prevenir troyanos y malware

Figura C. 16 Restricciones de Firewal

Ingrese la lista de puertos TCP necesarios de salida

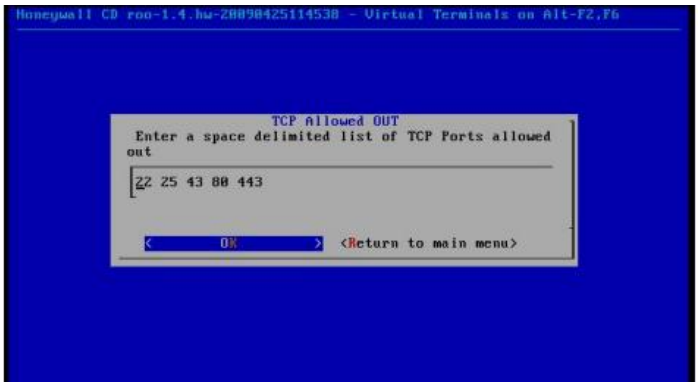


Figura C. 17 Puertos TCP de salida

Ingrese la lista de puertos UDP necesarios de salida.

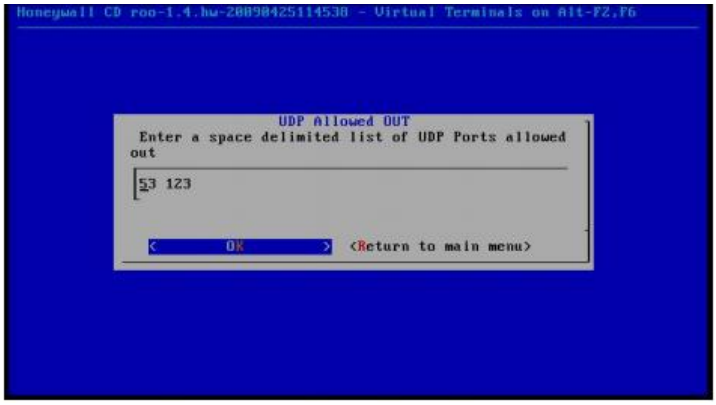


Figura. C.17. Puertos UDP de salida

- **Configuración del límite de Conexiones Permitidas**

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

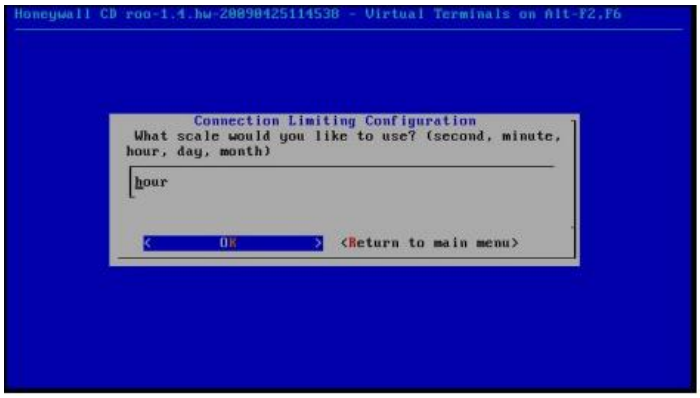


Figura. C.18. Límite de Conexiones (h, m, s)

Especificar el numero de Conexiones TCP que se permiten

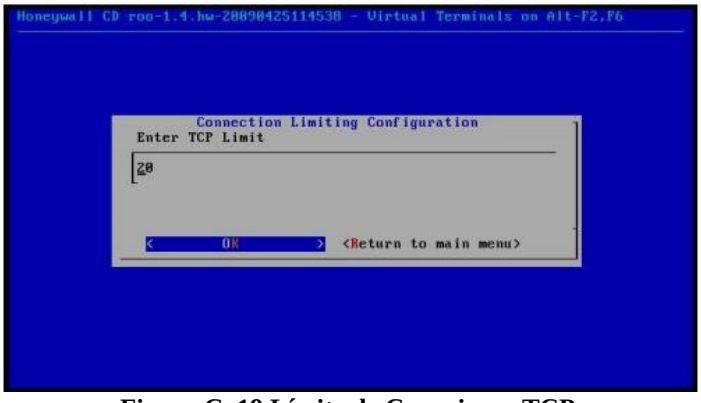


Figura C. 19 Límite de Conexiones TCP

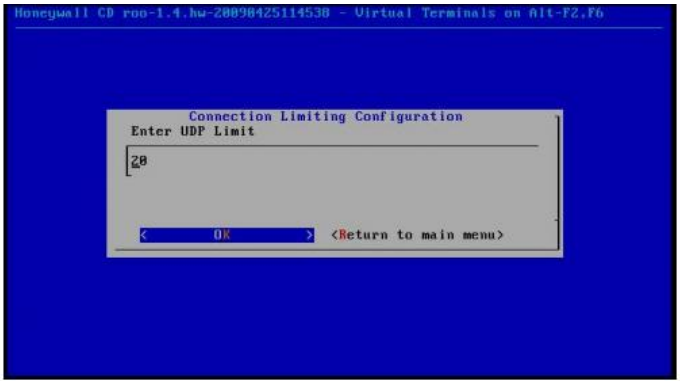


Figura C. 20 Límite de Conexiones UDP

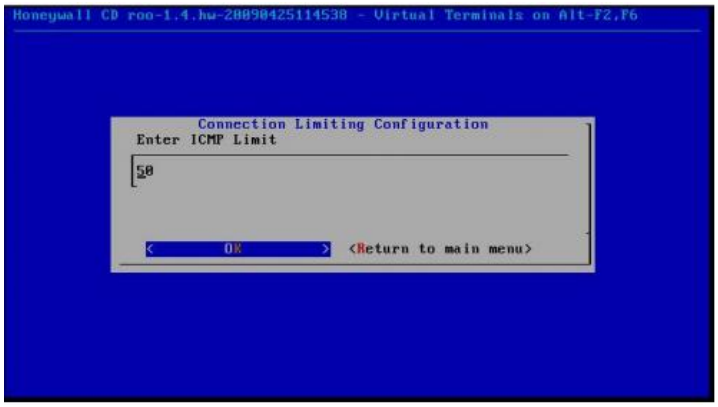


Figura C. 21 Límite de Conexiones ICMP

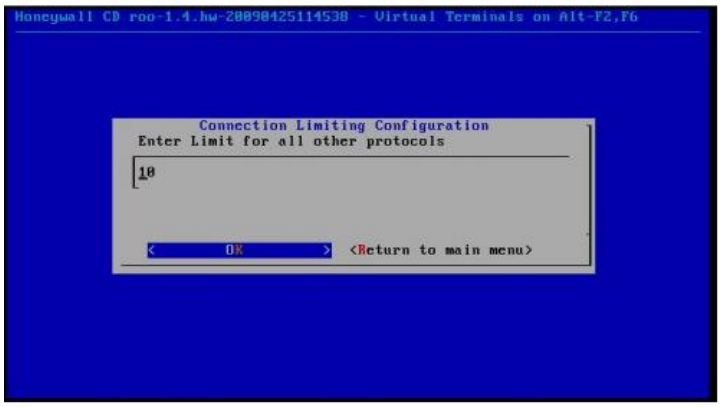


Figura. C.22. Límite de Conexiones otros Protocolos

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

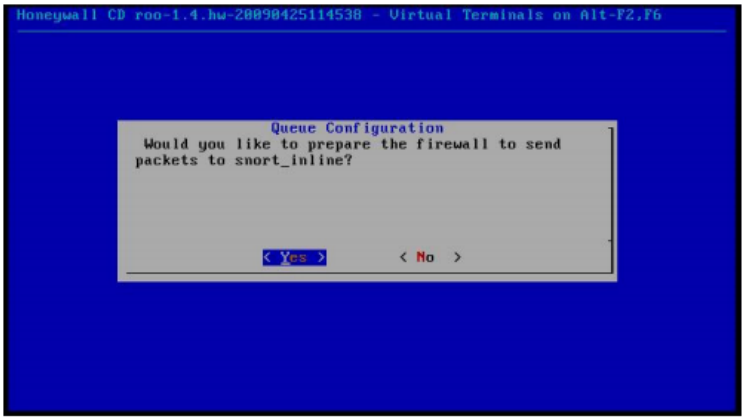


Figura. C.23. Activación de Snot-inline

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

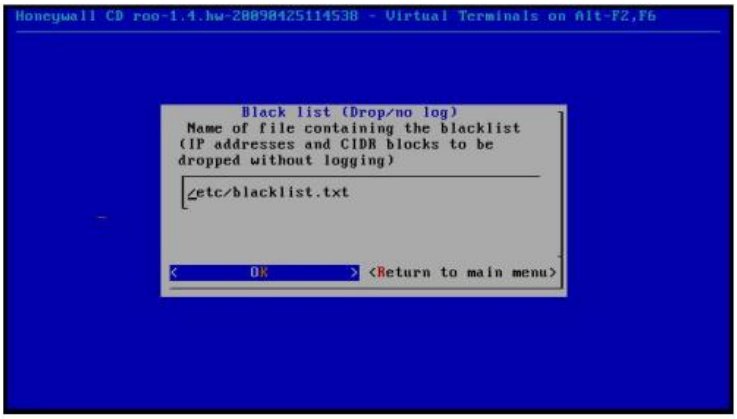


Figura. C.24. Dirección del Archivo Blacklist

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

Figura C. 25 Dirección del Archivo Whitelist

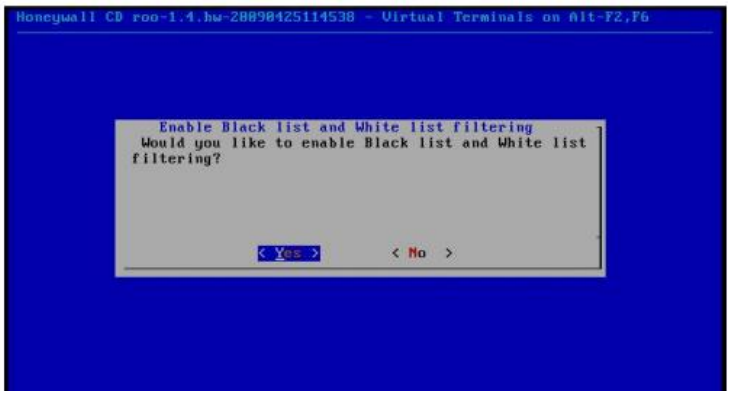


Figura C. 26 Filtrado de la lista Blanca y Negra

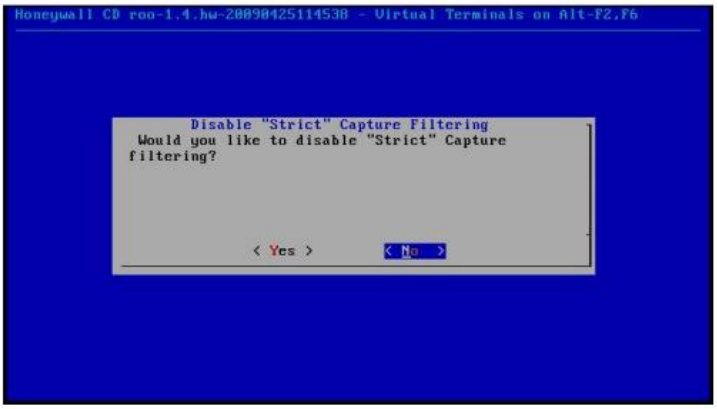


Figura C. 27 Habilitar "Strict" Capture Filtering

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

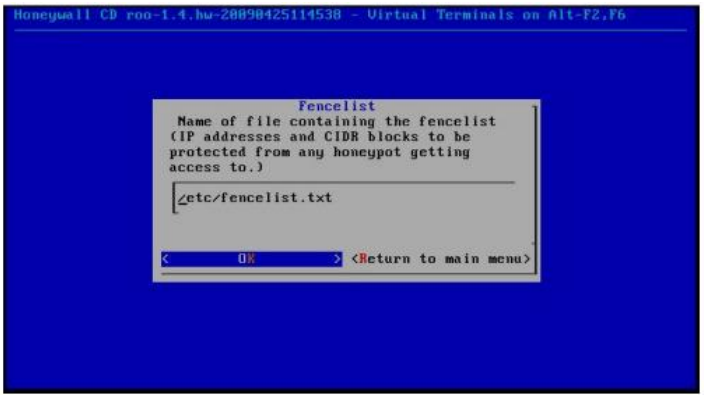


Figura C. 28 Nombre del Archivo de FENCELIST

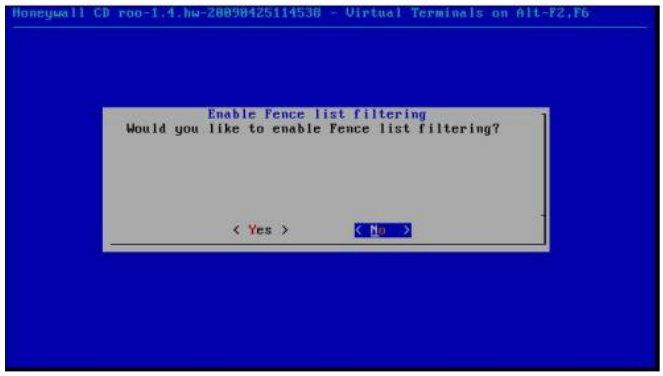


Figura C. 29 Habilitar FenceList

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

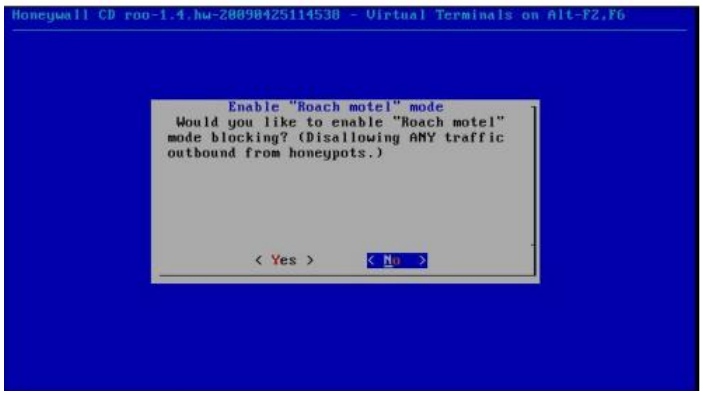


Figura C. 30 Habilitar Roach Motel

- **Configuración de DNS**

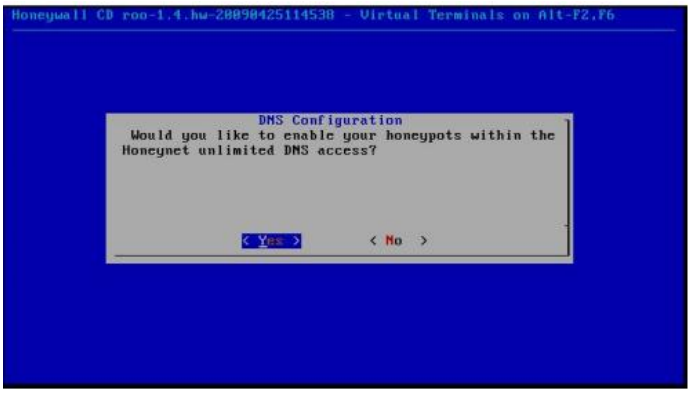


Figura C. 31 Configuración de los DNS para los Honeypots

Ingresar la lista de las direcciones IPs de los Honeypots

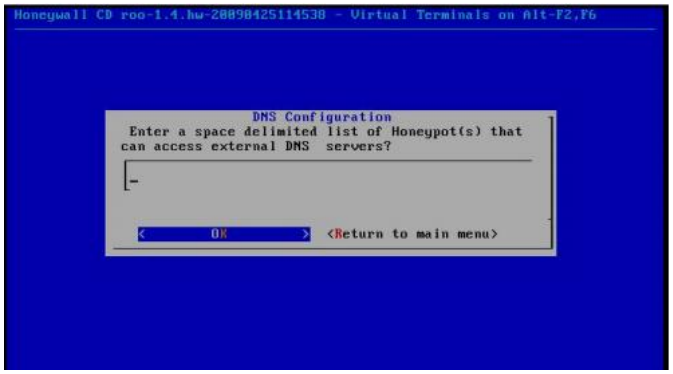


Figura C. 32 IPs de los Honeypots

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

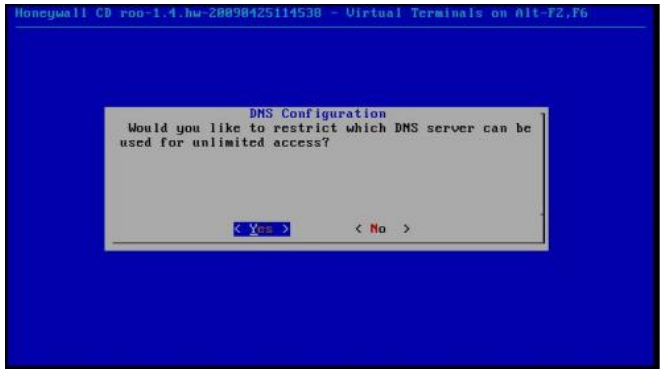


Figura C. 33 Configuración Servidor DNS

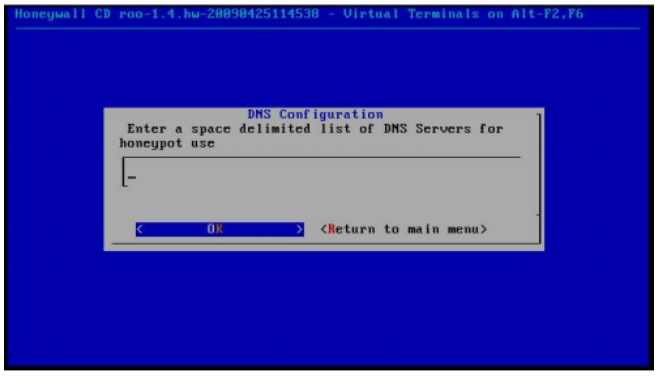


Figura C. 34 IP del servidor DNS para el Honeypot

- **Configuración de Alertas**

Figura C. 35 Configuración de alertas de mail

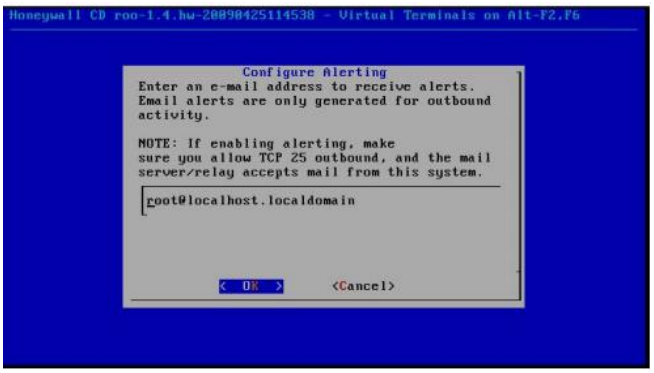


Figura C. 36 Correo electrónico usado para recibir las alertas

Figura C. 37 Finalización de la Configuración del Honeywall

ANEXO E

CONFIGURACION E INTALACION DE LOS SERVICIOS

- **Servidor DNS**

1. Instalar el servidor DNS mediante el siguiente comando:

   *yum install -y bind bind-chroot bind-libs *

2. En esta ruta */var/named/chroot/etc* se deberá crear el fichero "named.conf" y añadir al fichero el siguiente contenido:

```
options {
        directory "/var/named/";
        dump-file "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";

allow-recursion {
        127.0.0.1;
        10.1.28.0/22;
};

zone "." {
        type hint;
        file "named.ca";
};

zone "localhost" {
        type master;
        file "localhost.zone";
        allow-update { none; };
};

zone "deee.espe.edu.int.com" {
        type master;
        file "deee.espe.edu.int.zone";
        allow-update { none; };
};

zone "28.1.10.in-addr.arpa" {
```

```
        type master;
        file "1.1.192.in-addr.arpa.zone";
        allow-update { none; };
};
```

3. En la ruta */var/named/chroot/var/named* se crearan los ficheros de zona (deee.espe.edu.int.zone y 28.1.10.in-addr.arpa.zone) que serán invocados por named.conf

   - En el fichero deee.espe.edu.int.zone, se agrega el siguiente contenido:

```
$TTL 86400
@ IN SOA dns1.dee.espe.edu.int.com. root.deee.espe.edu.int.com. (
        2008061001; Numero de Serie
        28800; Tiempo de Refresco
        7200; Tiempo de Reintentos
        604800; Expiracion
        86400; Tiempo Total de Vida
)
@       IN      NS      dns1
@       IN      A       10.1.28. 200
dns1    IN      A       10.1.28. 200
```

   Donde: dns1 es el nombre del host que va a prestar este servicio

   - En el fichero 28.1.10.in-addr.arpa.zone, se agrega el siguiente contenido:

```
$TTL 86400
@       IN      SOA     dns1.tuDominio.com.     root.tuDominio.com. (
        2008061002; Numero de Serie
        28800; Tiempo de Refresco
        7200; Tiempo de Reintentos
        604800; Expiracion
        86400; Tiempo Total de Vida
)

@       IN      NS      dns1.deee.espe.edu.int.com.
```

```
200     IN      PTR     dns1.deee.espe.edu.int.com.
```

Donde: El numero **[200]** hace referencia al ultimo octeto de la dirección IP asignada a nuestro DNS, nos referimos a la dirección IP **10.1.28.200.**

4. Se configura el fichero */etc/sysconfig/network*, en el cual se debe agregar el nombre del equipo que desempeñara la función de servidor DNS, al final este fichero deberá verse de una forma similar a esta.

```
NETWORKING=yes
NETWORKING_IPV6=no
HOSTNAME=dns1.tuDominio.com
```

5. Finalmente se inicia el servidor DNS, utilizando el siguiente comando:
   service named start

- **Servidor DHCP**

1. Instalo 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 de Correo**

1. Instalar los siguientes paquetes haciendo uso del siguiente comando

yum install -y sendmail sendmail.cf dovecot cyrus-sasl cyrussasl-plain cyrus-sasl-md5 make m4

2. Configurar el fichero /etc/mail/access, el archivo debe quedar de la siguiente manera

 # By default we allow relaying from localhost...
Connect:localhost.localdomain RELAY
Connect:localhost RELAY
Connect:127.0.0.1 RELAY

#Nombre de su Dominio
Connect: deee.espe.edu.int.mx RELAY

#Nombre de su Equipo
Connect: dns1.deee.espe.edu.int.mx RELAY

#IP Local de su Servidor de correo
Connect: 10.1.28.200 RELAY

3. Configurar el fichero /etc/mail/local-host-names, el archivo debe debería quedar editado de la siguiente forma

   dns1.deee.espe.edu.int.mx
   deee.espe.edu.int.mx

4. Configurar el fichero /etc/mail/relay-domains, el archivo debe debería quedar editado de la siguiente forma

   dns1.deee.espe.edu.int.mx
   deee.espe.edu.int.mx

5. Configurar el fichero /etc/mail/sendmail.mc

   - Activar las interfaces de red para que sendmail envié correos desde cualquier IP.

     DAEMON_OPTIONS(`Port=smtp , Name=MTA')dnl

   - Enmascarar dominios para enviar correo con solo un dominio, para ello ubique las líneas y descomentando la línea eliminando la palabra **dnl** que se encuentra al principio de la línea, el resultado debe ser el siguiente.

     dnl MASQUERADE_AS(`mydomain.com')dnl
     FEATURE(masquerade_envelope)dnl
     FEATURE(masquerade_entire_domain)dnl

   - Habilitar el puerto 587 para el envió de correo, descomentando la línea eliminando la palabra **dnl** que se encuentra al principio de la línea, el resultado debe ser el siguiente.

     DAEMON_OPTIONS(`Port=submission, Name=MSA, M=Ea')dnl

   - Habilitar la autenticación de los usuarios de correo por el método plano, se encuentra habilitada por defecto pero es necesario descomentar las siguientes líneas:

     TRUST_AUTH_MECH(`EXTERNAL DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dnl

define(`confAUTH_MECHANISMS', `EXTERNAL GSSAPI DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dnl

6. Configuración del servidor Dovecot

   - Editar el fichero **/etc/dovecot.conf**, ubicar la siguiente línea

     #protocols = imap imaps pop3 pop3s

   - Borrar **imaps pop3s**, así como también la almohadilla de **"#",** el resultado deberá lucir de la siguiente manera:

     protocols = imap pop3

7. Crear las cuentas de correo mediante el siguiente comando

   useradd -s /sbin/nologin nombreDelsuario

8. Asignar contraseñas a las cuentas de correo, mediante los siguientes comandos

   passswd nombreDelsuario

   saslpasswd2 nombreDelsuario

9. Iniciar el servidor Sendmail

   service senmail start

10. Iniciar el servidor Dovecot

    service dovecot start

11. Iniciar el servidor de Autenticación

    service saslauthd start

- **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:
   /etc/init.d/vsftpd start

INDICE DE FIGURAS

INDICE DE TABLAS

GLOSARIO

AMDdnsfuckr: Es una herramienta que envía múltiples peticiones PTR (resolución inversa IP → dominio) de IPs aleatorias al servidor DNS.

AMDkillDNS: Es una herramienta que falsifica la memoria cache de servidor DNS.

Auto-rooters: Una herramienta que escanea un rango específico de red en busca de vulnerabilidades.

Backdoors: (Puerta trasera) Defecto en un software o página web que permite ingresar a un recurso que usualmente está restringida a un usuario ajeno

BSD: *Berkeley Software Distribution* (en español, "distribución de software berkeley") es un sistema operativo derivado del sistema Unix

Bug: Error de Software.

Centos: (Community ENTerprise Operating System) es un clon a nivel binario de la distribución Linux Red Hat Enterprise Linux RHEL

Crackers: Persona que viola la seguridad de un sistema informático de forma similar a como lo haría un hacker, el cracker realiza la intrusión con fines de beneficio personal o para hacer daño.

CPU: Central Processing Unit (unidad de proceso central), se pronuncia como letras separadas. La CPU es el cerebro del ordenador.

DHCP: Dynamic Host Configuration Protocol (Protocolo de configuración dinámica de ***host***) es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente.

DNS: Domain Name System o DNS (Sistema de nombres de dominio) es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada.

DoS: *(Denial of Service)* es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

Ethernet: Ethernet es un estándar de redes de computadoras de área local con acceso al medio por contienda CSMA/CD ("Acceso Múltiple por Detección de Portadora con Detección de Colisiones")

Exploid: Es una pieza de software, secuencia de comandos con el fin de automatizar el aprovechamiento de un error, fallo o vulnerabilidad.

Firewall: Un cortafuegos *firewall* en (idioma inglés) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Gateway: Puerta de enlace (Gateway) es un dispositivo, con frecuencia un ordenador, que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación

Hackers: Gente apasionada por la seguridad informática.

Honeyd: Es un Honeypot que simula redes con hosts activos con puertos y servicios abiertos, entonces se tienen redes simuladas levantadas para atraer atacantes a dichas redes.

Honeynet: Los Honeynet son un tipo especial de Honeypot de alta interacción que actúan sobre una red entera, diseñada para ser atacada y recobrar así mucha más información sobre posibles atacantes

Honeypot: Se denomina ***honeypot*** al software o conjunto de computadores cuya intención es atraer a atacantes, simulando ser sistemas vulnerables o débiles a los ataques.

Honeywall: Una Honeywall es un ordenador configurado para filtrar y observar el tráfico que generan uno o varios Honeypots protegiendo al resto de la subred de los ataques de los mismos.

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

HTML: HyperText Markup Language (*Lenguaje de Marcado de Hipertexto*), es el lenguaje de marcado predominante para la elaboración de páginas web.

HTTP: Hypertext Transfer Protocol o HTTP (en español *protocolo de transferencia de hipertexto*) es el protocolo usado en cada transacción de la World Wide Web.

IDS: Sistema de detección de intrusos (*Intrusion Detection System*) es un programa usado para detectar accesos no autorizados a un computador o a una red.

IPS: (Intrusion Prevention System o Sistema de Prevención contra Intrusiones) evita que intrusiones y ataques conocidos puedan afectar a la red corporativa.

Kernel: Es un software que actúa de sistema operativo.

Linux: Es un núcleo de sistema operativo libre tipo Unix. Linux está licenciado bajo la GPL v2 y está desarrollado por colaboradores de todo el mundo.

Logs: Es un registro oficial de eventos durante un rango de tiempo en particular.

MySQL: Es un sistema de gestión de base de datos relacional, multihilo y multiusuario con más de seis millones de instalaciones.

NTOP: (Network TOP) es una herramienta que no puede faltar al administrador de red, porque permite monitorizar en tiempo real los usuarios y aplicaciones que están consumiendo recursos de red en un instante concreto

Perl: Es un lenguaje de programación, con características del lenguaje C, del lenguaje interpretado shell, AWK, sed, Lisp y, en un grado inferior, de muchos otros lenguajes de programación.

Pharming: Es la explotación de una vulnerabilidad en el software de los servidores DNS (*Domain Name System*).

Phishing: Es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas.

Port Mirroring: Port mirroring es una función que tienen los Switches para copiar todo el tráfico de un puerto específico a otro puerto.

Rack: Es un bastidor destinado a alojar equipamiento electrónico, informático y de comunicaciones.

RAM: *Random access memory*, un tipo de memoria de ordenador a la que se puede acceder aleatoriamente

Rootkit: Es una herramienta o un grupo de ellas, que tiene como finalidad esconderse a sí misma y esconder

	otros programas, procesos, claves de registro, y puertos que permiten al intruso mantener el acceso a un sistema para remotamente comandar acciones.
Router:	Es un dispositivo de hardware para interconexión de red de ordenadores que opera en la capa tres (nivel de red) del modelo OSI.
SEC:	Simple Event Correlator, analiza un fichero, una canalización con nombre o la entrada estándar y mediante expresiones regulares, reconoce eventos, de modo que cuando se produce una coincidencia con un patrón especificado puede ejecutar comandos del sistema.
Slowloris:	Es un cliente HTTP que permite desde un solo sistema saturar determinados servidores web, siendo uno de los destacados Apache tanto en sus versiones 1.x como en las 2.x.
SMTP:	(Simple Mail Transfer Protocol) Protocolo Simple de Transferencia de Correo, es un protocolo de la capa de aplicación.
Sniffer:	Es un software destinado para detectar tramas en la red.
Snooping:	El snooping tiene como objetivo obtener información de una red a la que están conectados sin modificarla
Switch:	Es un dispositivo digital de lógica de interconexión de redes de computadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI.
VirtualBox:	Es un software de virtualización para arquitecturas x86.
Virtualización:	Se refiere a la abstracción de los recursos de una computadora, crea una capa de abstracción entre el hardware de la máquina física (host) y el sistema operativo de

	la máquina virtual (virtual machine, guest), siendo un medio para crear una versión virtual de un dispositivo o recurso.
VLAN:	*Virtual LAN*, 'Red de Área Local Virtual' es un método de crear redes lógicamente independientes dentro de una misma red física.
Vmware:	Es un sistema de virtualización por software.
VPN:	Red privada virtual (*Virtual Private Network*) es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.
Walleye:	Interfaz gráfica del Proyecto Honeynet.

CERTIFICACION

Certificamos que el presente trabajo de graduación, titulado DISEÑO E IMPLEMENTACION DE UNA HONEYNET PARA LA RED DEL DEPARTAMENTO DE ELECTRICA Y ELECTRONICA (DEEE) UTILIZANDO VIRTUALIZACION, fue realizados por los estudiantes Andrea Albán y Cristian Palacios

Ing. Carlos Romero	Ing. Fabián Sáenz
DIRECTOR	CODIRECTOR