



**UNIVERSIDAD TÉCNICA DE AMBATO**  
**FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL**  
**CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E**  
**INFORMÁTICOS.**

**Tema:**

---

**“HONEYPOT COMO HERRAMIENTA DE PREVENCIÓN Y DETECCIÓN DE  
CIBERATAQUES EN LAS REDES DE DATOS DE LA FACULTAD DE  
INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL.”**

---

Trabajo de Graduación. Modalidad: Proyecto de Investigación, presentado previo la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos.

**SUBLÍNEA DE INVESTIGACIÓN:** Seguridad Informática.  
**AUTOR:** Vargas Paredes Javier Santiago.  
**PROFESOR REVISOR:** Ing. José Vicente Morales Lozada M. Sc.

Ambato - Ecuador

Julio - 2015

## **APROBACIÓN DEL TUTOR**

En mi calidad de Tutor del Trabajo de Investigación sobre el Tema: **“HONEYPOT COMO HERRAMIENTA DE PREVENCIÓN Y DETECCIÓN DE CIBERATAQUES EN LAS REDES DE DATOS DE LA FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL.”**, del señor Vargas Paredes Javier Santiago, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad con el numeral 7.2 de los Lineamientos Generales para la aplicación de Instructivos de las Modalidades de Titulación de las Facultades de la Universidad Técnica de Ambato

Ambato, julio del 2015

TUTOR

---

Ing. Vicente Morales L., Mg.

## AUTORÍA

El presente Proyecto de Investigación titulado: “**HONEYPOT COMO HERRAMIENTA DE PREVENCIÓN Y DETECCIÓN DE CIBERATAQUES EN LAS REDES DE DATOS DE LA FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL**”, es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, julio del 2015

---

Javier Santiago Vargas Paredes

CC: 1804381679

## **DERECHOS DE AUTOR**

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este Trabajo de Titulación como documento disponible para la lectura, consulta y procesos de investigación.

Cedo los derechos de mi Trabajo, con fines de difusión pública, además autorizo su reproducción dentro de las regulaciones de la Universidad.

Ambato, julio del 2015

---

Javier Santiago Vargas Paredes

CC: 1804381679

## APROBACIÓN DEL TRIBUNAL DE GRADO

La Comisión Calificadora del presente trabajo conformada por los señores docentes Ing. Franklin Mayorga M., Mg. e Ing. David Guevara A., Mg., revisó y aprobó el Informe Final del Proyecto de Investigación titulado “**HONEYPOT COMO HERRAMIENTA DE PREVENCIÓN Y DETECCIÓN DE CIBERATAQUES EN LAS REDES DE DATOS DE LA FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL.**”, presentado por el señor Javier Santiago Vargas Paredes, de acuerdo al numeral 9.1 de los Lineamientos Generales para la aplicación de Instructivos de las Modalidades de Titulación de las Facultades de la Universidad Técnica de Ambato.

---

Ing. Vicente Morales L., Mg.

PRESIDENTE DEL TRIBUNAL

---

Ing. Franklin Mayorga M., Mg.

DOCENTE CALIFICADOR

---

Ing. David Guevara A., Mg.

DOCENTE CALIFICADOR

## **DEDICATORIA**

*El presente proyecto se lo dedico a mi madre, por su apoyo fundamental en mi continuo crecimiento profesional, por compartir conmigo cada alegría y por constituir un pilar esencial en mi vida.*

*“Escribiremos nuevas reglas esta es la primera de ellas está prohibido prohibir”. **Enrique Bunbury.***

*Javier Santiago Vargas Paredes*

## **AGRADECIMIENTO**

*Quiero expresar mis más sinceros agradecimientos a mi madre y mi abuelito, gracias a ellos soy una persona de bien por inculcarme siempre buenos valores y por demostrarme que lo imposible no existe.*

*A la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato, por ser una guía en mi formación en el ámbito profesional, ético y moral.*

*Así como también a todos y cada uno de los docentes quienes a lo largo de mi formación académica permitieron que un estudiante más sepa contar con sus valiosas aportaciones y conocimiento en el aprendizaje continuo.*

*Al Ing. Vicente Morales, por su valiosa amistad, ayuda y colaboración en la presente investigación.*

*A todos quienes supieron brindarme su apoyo, mis más sincero y eterno gratitud a cada uno de ellos.*

*Javier Santiago Vargas Paredes*

## Índice de Contenidos

CAPÍTULO 1.....	1
EL PROBLEMA.....	1
1.1 Tema.....	1
1.2 Planteamiento del problema.....	1
1.3 Delimitación.....	2
1.4 Justificación.....	3
1.5 Objetivos .....	4
1.5.1 General .....	4
1.5.2 Específicos.....	4
CAPÍTULO 2.....	5
MARCO TEÓRICO .....	5
2.1 Antecedentes Investigativos.....	5
2.2 Fundamentación teórica .....	6
2.3 Propuesta de Solución .....	14
CAPÍTULO 3.....	15
METODOLOGÍA.....	15
3.1 Modalidad de la investigación .....	15
3.2 Recolección de información.....	15
3.3 Procesamiento y análisis de datos .....	15
3.4 Desarrollo del proyecto .....	16
CAPÍTULO 4.....	18
DESARROLLO DE LA PROPUESTA .....	18
4.1 Análisis.....	18



4.2 Determinar las políticas y herramientas aplicables .....	21
4.3 Diseño de una Honeynet .....	33
4.4 Procesos y Herramientas de la Honeynet.....	51
4.5 Resúmenes presentados por el Honeypot (Honeywall) .....	68
CAPÍTULO 5.....	75
CONCLUSIONES Y RECOMENDACIONES .....	75
5.1 Conclusiones .....	75
Bibliografía .....	77
ANEXO A1 .....	78
ANEXO A2 .....	85

## Índice de Gráficos

Gráfico 2.2. 1 Honeypot diagrama general.....	8
Gráfico 2.2. 2 Honeypot como equipo físico en la red .....	9
Gráfico 2.2. 3 Diagrama Honeynet .....	10
Gráfico 2.2. 4 Modelo evaluación de riesgos .....	11
Gráfico 2.2. 5 HoneyWall.....	13
Gráfico 2.2. 6 Análisis del atacante en la red (Kali Linux) .....	14
Gráfico 4.2. 1 Políticas de Seguridad .....	22
Gráfico 4.2. 2 Modelo red de datos de la FISEI - .....	26
Gráfico 4.2. 3 Análisis de vulnerabilidades Avira OASYS.....	29
Gráfico 4.2. 4 Honeynet Básica en una red local.....	29
Gráfico 4.2. 5 Servidor en la red de datos. ....	30
Gráfico 4.2. 6 Medio de acceso para su control.....	30
Gráfico 4.2. 7 Software VMWare.....	31
Gráfico 4.2. 8 Software VirtualBox .....	31
Gráfico 4.2. 9 Software Qemu .....	32
Gráfico 4.2. 10 Modulo User-Mode Linux .....	32
Gráfico 4.3. 1 Red Honeynet Implementada .....	34
Gráfico 4.3. 2 Honeypot virtual configurado en la red.....	37
Gráfico 4.3. 3 Adaptador1 de red Honeypot.....	38
Gráfico 4.3. 4 Adaptador2 de red Honeypot.....	38
Gráfico 4.3. 5 Adaptador3 de red Honeypot.....	39
Gráfico 4.3. 6 Menú principal Honeywall .....	47
Gráfico 4.3. 7 Menú Informativo del funcionamiento del Honeywall .....	47
Gráfico 4.3. 8 Menú administrativo del Honeywall. ....	48
Gráfico 4.3. 9 Menú primordial de configuración Honeywall .....	49
Gráfico 4.3. 10 Administrador de interfaz web del Honeywall.....	50

Gráfico 4.3. 11 Ventana principal de administración. ....	50
Gráfico 4.4. 1 Honeywall como intermediaron de conexión. ....	55
Gráfico 4.4. 2 Pruebas de conectividad. Kali Linux .....	56
Gráfico 4.4. 3 Escaneo mediante nmap -O. ....	57
Gráfico 4.4. 4 Escaneo mediante nmap -sV.....	57
Gráfico 4.4. 5 Escaneo mediante nmap -sS. ....	58
Gráfico 4.4. 6 Valores obtenidos en el análisis nmap.....	59
Gráfico 4.4. 7 Tabulación de resultados por calendario. ....	59
Gráfico 4.4. 8 Metasploit como herramienta de explotación de vulnerabilidades. ....	60
Gráfico 4.4. 9 Primer resultado obtenido por el Honeywall. ....	61
Gráfico 4.4. 10 Pruebas de conectividad. WindowsXP.....	61
Gráfico 4.4. 11 Resultado diagrama de envió excesivo de paquetes. ....	62
Gráfico 4.4. 12 Honeywall comprometido por varios accesos en la red. ....	62
Gráfico 4.4. 13 Listas de conexiones hacia y desde el Honeywall.....	66
Gráfico 4.4. 14 Administrador de las reglas de Snort.....	67
Gráfico 4.5. 1 Modulo para guardar los análisis presentados en el Honeywall.....	68
Gráfico 4.5. 2 Resultado ARP .....	69
Gráfico 4.5. 3 Estadísticas ARP.....	70
Gráfico 4.5. 4 Resultados ICMP .....	71
Gráfico 4.5. 5 Estadísticas ICMP.....	71
Gráfico 4.5. 6 DNS acceso.....	72
Gráfico 4.5. 7 DNS acceso 2.....	72
Gráfico 4.5. 8 Estadística DNS .....	73

## Índice de Tablas

Tabla 4.2. 1 Honeypots experimentales .....	25
Tabla 4.2. 2 Puertos y Protocolos .....	27
Tabla 4.2. 3 Simplicidad de la red .....	30
Tabla 4.3. 1 Honeypot configuración de red. ....	39
Tabla 4.3. 2 Configuración administrador Honeywall. ....	40
Tabla 4.4. 1 Equipamiento necesario para la red Honeynet .....	51
Tabla 4.4. 2 Software utilizado monitoreo y control .....	52

## **Resumen**

El presente proyecto analiza las posibles vulnerabilidades e inseguridades presentes en las redes de datos y sistemas informáticos de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, FISEI, implementando una tecnología conocida como Honeypot, herramienta que simula servicios y aplicaciones vulnerables en una red trampa llamada HoneyNet, a este tipo de tecnologías se las conoce como Sistemas de Detección de Intrusos (IDS), utilizados para monitorear los eventos que ocurren en un sistema informático en busca de intentos de intrusión en la red de datos; todo el tráfico en la red analizado, nos permite evaluar e incrementar reglas de seguridad informática entre los usuarios internos y externos de la red de datos. Además en este trabajo se han analizado los resultados del Honeypot como actividades de un hacker o atacante accediendo a la red, a partir de estas alertas el administrador del sistema puede tomar medidas preventivas.

## **Abstract**

The present project of investigation, analyzes the possible vulnerabilities and present insecurities in the data networks and information systems of the Facultad de Ingeniería en Sistemas, Electrónica e Industrial, FISEI, implementing a technology known as Honeypot, tool that simulates services and or vulnerable applications in a network trap called Honeynet to this type of technologies they are known as Intrusion Detection System (IDS) used to monitor the events occurring in a computer system for intrusion attempts in the network data; all traffic on the network analyzed, allows us to evaluate security rules between internal and external users of the data network. Also in this paper have analyzed the results of Honeypot as activities of a hacker or attacker accessing the network from these alerts the system administrator can take preventive measures.

## Glosario de términos y acrónimos

<b>Ciberataques:</b>	Ataques realizados por medio de computadores o dispositivos conectados en una red local o por Internet.
<b>IDS:</b>	Un Sistema de detección de intrusos, su funcionalidad es detectar accesos no permitidos a un computador o en una red de datos.
<b>VPNs:</b>	Grupo de redes o red privada virtual.
<b>ACL:</b>	Son unas listas que permiten el control de acceso al medio, para separar los niveles de privilegio.
<b>DDoS:</b>	En seguridad informática, un ataque de denegación de servicios.
<b>Honeypot:</b>	Denominado por ser un software o computadores, que simulan ser un sistema vulnerable, así distraendo al atacante.
<b>Firewall:</b>	Sistema de protección en una red, diseñado para bloquear o controlar el acceso no autorizado, permitiendo conexiones de confianza.
<b>Wrappers:</b>	Sistema de alto nivel de seguridad, la funcionalidad principal es permitir o bloquear los servicios o procesos del Servidor o Sistema.
<b>MD5:</b>	Algoritmo que usa un código propio de archivo para su protección.
<b>SHA:</b>	Un conjunto de funciones o scripts diseñados para proteger una aplicación o un dispositivo, con la implementación de algoritmos.
<b>PGP:</b>	Sistema desarrollado para resguardar la información en las comunicaciones de datos.
<b>NIDS:</b>	Un sistema que permite la detección de intrusiones en una red local o una red virtual.
<b>HIDS:</b>	Un sistema que detecta posibles intrusiones en las maquinas conectadas en una red.
<b>Honeynet:</b>	Es un grupo o un conjunto de Honeypots de alta interacción en una red diseñada para ser vulnerada, puede ser un modelo experimental para conocer los tipos de ataques nuevos que se pueden producir en un Sistema determinado.

<b>SNMP:</b>	Protocolo de administración de red, utilizado para un escaneo y diagnóstico de la red.
<b>CDROM:</b>	Contiene la información, de un Sistema de arranque e instalación, no puede ser utilizado para regrabar la información generada en la instalación.
<b>IPsec:</b>	Grupo de protocolos, configurados para asegurar las conexiones en una red, seguridad en IP.
<b>Logs:</b>	Registros temporales de la actividad de un software o un sistema en producción, el almacenamiento es generado por el comportamiento del mismo, pueden ser registros informativos, alertas o configuraciones necesarias.
<b>AAA:</b>	Tres funciones principales; autenticación, autorización y contabilización.
<b>GNU:</b>	Sistema operativo de tipo Unix, acrónimo recursivo que significa "GNU No es Unix".
<b>FDL:</b>	Free Software Foundation.
<b>GUI:</b>	Una interfaz gráfica de usuario, para la interacción con el sistema.
<b>HWCTL:</b>	Comando o herramienta para la ejecución de las órdenes para la administración del Honeywall.
<b>Walleye:</b>	Modulo de administración del Honeywall, permite el uso de una interfaz web.



<b>NetworManager:</b>	Servicio de administración de red, configurado en CentOS 6.5.
<b>DNS:</b>	Un servicio o sistema de nombres de dominio, configurado en el servidor local.
<b>SSH:</b>	Protocolo de comunicación segura para permitir o denegar las conexiones entrantes y salientes.
<b>HTTP:</b>	Protocolo para la transferencia de hipertexto.
<b>Nmap:</b>	Una herramienta para en análisis de redes de datos, en seguridad informática es utilizada para el escaneo de puertos abiertos en un servidor y advertir al administrador de red.
<b>Snort:</b>	Un sniffer de paquetes en una red, permite detectar intrusos basado en sus reglas de configuración, uso el registró o logs para poder monitorizar la red y las posibles intrusiones.
<b>Metasploit:</b>	Conjunto de herramientas para análisis de vulnerabilidades y para ataques informáticos con intención maligna o en escenarios controlados.
<b>Hosts:</b>	Termino referenciado para la descripción de máquinas o sistemas anfitriones en una red.
<b>Wireshark:</b>	Software que permite el escaneo de la red completa, presentando la información de manera detallada, permite analizar todo tipo de puerto y paquete, o configuración en la red de datos.

## Introducción

Un Honeypot proviene de varios estudios en el área de Seguridad Informática, para el análisis se simula un ambiente controlado de una red de datos, con la finalidad de distraer al atacante del sistema anfitrión real y a su vez obtener información del mismo analizando los métodos y técnicas utilizadas para acceder a un recurso o servicio de la red de datos [3-4].

La información que circula en una red de datos puede ser manipulada por expertos en el área de redes, pero a su vez existen atacantes que usan esa información a su conveniencia, un usuario en una computadora dentro de una red de datos ingresa a un sistema de aplicación a través de Internet o localmente, el atacante puede usar un software que permite capturar tramas de la red robando información de gran importancia. La seguridad informática, eje fundamental en la protección de la información, contempla las vulnerabilidades que se puede presentar en su red de datos o estaciones de trabajo.

El informe final del presente trabajo de investigación se orienta a la seguridad informática de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, estructurado en capítulos, que proporcionan una mejor comprensión del contenido del mismo.

En el **CAPÍTULO 1**, se identifica y evidencia problemas sobre la seguridad informática el **CAPITULO 2** presenta antecedentes investigativos sobre ciberataques y tecnologías orientadas a la seguridad informática. Para el **CAPITULO 3** siguiendo los objetivos del trabajo se especifica la modalidad de investigación a utilizar; estos capítulos ayudan a la elaboración del **CAPITULO 4** que detalla la herramienta utilizada para la detección y prevención de vulnerabilidades en las redes de datos de la FISEI, y por último se encuentra el **CAPITULO 5** aquí se muestra a qué conclusiones se ha llegado con la investigación realizada, además algunas recomendaciones según los resultados obtenidos en el proyecto de investigación.

Toda la investigación se fundamenta en una fuente **Bibliografía** con la cual se ha recolectado información necesaria para la investigación, como también los **Anexos** de configuraciones adicionales y resultados obtenidos en el proyecto de investigación.

# CAPÍTULO 1

## EL PROBLEMA

### 1.1 Tema

Honeypot como herramienta de prevención y detección de ciberataques en las redes de datos de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

### 1.2 Planteamiento del problema

Las redes de datos de comunicación dentro de la Universidad Técnica de Ambato consta de diferentes servicios a estudiantes, académicos, personal administrativo, investigadores e incluso a la sociedad en general, todo esto englobado en el uso de la red inalámbrica o física, considerando los dispositivos de conexión a la red local e Internet, el aplicar una política de seguridad condicional en el uso de la red puede constituir un problema.

Existe un conjunto de mecanismos o sistemas de protección de las redes de la Facultad, donde se puede encontrar, firewalls, listas de control de acceso (ACL), redes privadas virtuales (VPNs), sistemas de detección de intrusos (IDS), entre otros. Los cuales forman parte de un todo que ayuda a ampliar la seguridad de los sistemas de seguridad.

Para poder implementar las reglas concretas en firewalls, IDSs y demás medios de prevención, el administrador de la red debe tener un enfoque minucioso de los tipos de ataques a los que su red de datos puede verse afectada. El uso de una tecnología llamada Honeypots permite conocer con detalle los ataques y vulnerabilidades de las redes, con la técnica determinada “Conoce a tu Atacante” [1].

El fácil acceso a la red, ha contribuido en una evolución de las técnicas de ataques existentes, generando cambios en los escenarios típicos causantes de amenazas para cualquier sistema que preste sus servicios a través de Internet, por ejemplo en la Universidad Pontificia Bolivariana (Colombia), la seguridad informática de los sistemas de

las Oficinas de Registro Académico, fue deliberadamente vulnerada directamente usando equipos del mismo departamento, sin saber que fue la portátil de un estudiante, causante de este tipo de delito informático [2].

El contar con una información detallada de las actividades de intrusos que ingresan a sus redes es crucial, puesto que facilita el tomar medidas preventivas sobre el ataque o el atacante, además de poder actualizar las políticas de seguridad, para evitar réplicas o ataques con patrones similares, también proporcionará información detallada sobre las vulnerabilidades de sistemas que se puede suponer que aún no han sido afectadas. Todos buscamos algo simple y que funcione en cualquier plataforma, si el sistema afectado es un servicio significativo, no debe ser desconectado por ejemplo, un Servidor de Base de Datos. Actualmente la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, no cuenta con un sistema de seguridad informático que proteja la información, por lo que está expuesto a constantes ataques y sin que el administrador se informe de los Delitos Informáticos.

Los Delitos Informáticos más comunes que se pueden presentar son:

- Falsificación de información. Por ejemplo, un usuario ajeno al sistema puede infringir en un sistema y lograr acceder al académico, modificar calificaciones, y conseguir pasar o aprobar una materia, un empleado puede aumentar presupuestos asignados, entre otros.
- Ataques de denegación del servicio (DDoS).
- Ataques a Servidores por conexiones ajenas (en otras instituciones o países), de tal manera que no se pueda investigar el origen de los ataques o atacantes.

### **1.3 Delimitación**

- **Área académica:** Hardware y Redes.
- **Línea de investigación:** Sistemas Administradores de Recursos.
- **Sublínea de investigación:** Seguridad Informática.

- **Delimitación temporal:** La presente investigación se desarrollará en un periodo de seis meses comprendidos desde la fecha de aprobación de Consejo Directivo.
- **Delimitación espacial:** La presente investigación se realizará en la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato.

#### 1.4 Justificación

Es importante destacar que la Seguridad de la Información tiene como fin la protección de la información y de los sistemas de la información del acceso, uso, divulgación, interrupción o destrucción no autorizada.

Actualmente la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, se ha propuesto identificar, las inseguridades que se pueden encontrar en las redes de datos y los sistemas informáticos, teniendo como limitación principal las seguridades de nivel administrativo, pero no a nivel general, acorde a las necesidades de la Facultad, siendo un medio de control crítico para la misma. El uso de Honeypots como herramienta de investigación, consiste en el diseño de una red Honeynet para ser comprometida por intrusos, además para estudiar las técnicas utilizadas por los intrusos que han conseguido el acceso, consiguiendo así implementar una solución que permita contrarrestar los problemas de seguridad informática dentro de la FISEI.

Este proyecto es **factible** realizarlo en primera instancia por ser parte de una investigación del área de redes de la Universidad Técnica de Ambato, con el tema *“Implantación de una Honeynet para la optimización de la seguridad de la información en los Servidores de la Universidad Técnica de Ambato.”*.

El Tema a investigarse es de gran **importancia**, ya que se tendrá un mejor control sobre las seguridades informáticas de la Facultad, siendo esto el aspecto más importante y de mayor prioridad, pretendiendo facilitar y agilizar la administración de las redes de datos y sistema informático, donde se presenta recomendaciones de cómo evitar posibles Delitos Informáticos y resguardar la Seguridad Informática dentro de la Facultad.

Es **útil** debido a que se suministrará una herramienta, capaz de controlar y detener las amenazas que se pueden presentar, lo cual beneficia a estudiantes, docentes, personal administrativo y todos quienes interactúen directa e indirectamente con las redes de datos de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato.

## **1.5 Objetivos**

### **1.5.1 General**

- Implementar un Honeypot como herramienta de prevención y detección de ciberataques en las redes de datos de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

### **1.5.2 Específicos**

- Analizar las herramientas de detección de intrusos actualmente utilizadas en la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.
- Determinar las políticas y herramientas aplicables en la identificación de vulnerabilidades.
- Elaborar el diseño preliminar de una HoneyNet.
- Documentar los procesos y herramientas usados en la implantación de la HoneyNet.
- Presentar el análisis realizado por la herramienta Honeypot en la FISEI.

## CAPÍTULO 2

### MARCO TEÓRICO

#### 2.1 Antecedentes Investigativos

Las primeras reseñas de los Honeypot vienen desde 1990 en el libro publicado “El huevo del cuco” de Clifford Stolls el cual fundamento a “The HoneyNet Project” una organización dedicada a la investigación de sistemas o mecanismos de prevención y detección de intrusos, esta investigación se tornó a la seguridad informática y más concretamente en el rol de los sistemas de detección de intrusos (IDS). Hoy en día son conocidos los constantes ataques que sufren los Servidores y redes de computadores de las compañías más importantes del mundo, además las diferentes vulnerabilidades que se presentan en las páginas Web y Sistemas Informáticos.

A nivel universal existe un proyecto de investigación del uso de Honeypots en redes HoneyNet empresariales con el tema: “Reino Unido HoneyNet Project Estado Capítulo Anual Para 2011/2012” [3].

Como antecedentes investigativos se encontró un Trabajo de Graduación. Modalidad: **SEMINARIO de Graduación** en la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato con el tema “Sistemas MULTI-AGENTE para la detección de ataques en los entornos dinámicos y distribuidos de la Empresa Importadora REPCOPY”, concluyendo que: “En el Área de Tecnologías Informática existe muchos mecanismos de salvaguardar la información, el principal riesgo es la falta de conocimiento sobre estos, ya que día a día aparecen nuevas herramientas de monitoreo de la red al igual que aparecen las amenazas.” [4].

Actualmente la comunicación entre computadores ha cobrado una importancia vital en el mundo de la seguridad informática y el volumen de redes conectadas entre sí a lo largo del mundo supera cualquier expectativa inicial. La importancia de los datos que una empresa mueve a lo largo de sus canales de información es considerable y por ello las empresas invierten gran cantidad de recursos económicos y humanos para resguardar su seguridad, en

la actualidad, se continúa con la investigación y se plantean nuevas aplicaciones y proyectos como el Honey-Droid un Smartphone HoneyPot [5].

## **2.2 Fundamentación teórica**

### **Técnicas orientadas a la seguridad informática**

- **Sistemas de detección de intrusos:** son sistemas que consienten analizar las bitácoras de los sistemas en investigación de patrones de comportamiento o sucesos que puedan considerarse susceptibles, sobre la base de la información con la que han sido anticipadamente sustentados. Pueden ser terminales de control. [6]
- **Sistemas a conexión de red:** analizan las conexiones que se intentan instituir en una red o equipo en particular, capaces de efectuar una acción sobre la base de métricas como: inicio y grado de la conexión, servicio solicitado, permisos, entre otros. Las gestiones que pueden comenzar desde el bloqueo de la conexión hasta alerta al administrador de la red. En esta categoría están los cortafuegos (Firewalls) y los servicios de red (Wrappers) [6].
- **Sistemas de análisis de vulnerabilidades:** sistemas en busca de vulnerabilidades acreditadas anticipadamente, pueden ser utilizados tanto por usuarios autorizadas como por usuarios que buscan acceso no permitido al sistema [6].
- **Sistemas de protección a la integridad de información:** sistemas que mediante criptografía o sumas de verificación tratan de aseverar que no ha habido variaciones negativas en la información que se pretende proteger. Ejemplos son aplicaciones que efectúan algoritmos como Message Digest (MD5), o bien sistemas que manejan varios de ellos como programas de cifrados, Pretty Good Privacy (PGP), sistemas de protección a la privacidad Tripwire y DozeCrypt [6].
- **Sistemas de protección a la privacidad de la información:** herramientas que utilizan criptografía para asegurar que la información sólo sea visible para quien tiene autorización. Su aplicación se realiza primariamente en las comunicaciones entre



dos identidades. Dentro de este tipo de software aplicativo se pueden mencionar a Pretty Good Privacy (PGP), y los Certificados Digitales.

### **Sistema de detección de intrusos (IDS)**

Un sistema de detección de intrusos, se utiliza para detectar intrusos o posibles intrusiones en un entorno observado [6]. Dos lugares posibles para poner en práctica un mecanismo de detección de intrusos:

- Sistema de detección de intrusiones de red (NIDS)
- Sistemas de detección de intrusiones en el host (HIDS)

### **Mecanismo de un IDS**

Un IDS de red detecta patrones de ataque conocidos basándose en una firma, por lo tanto un IDS tiene dos habilidades importantes: La primera sirve para inspeccionar los paquetes en una trama de red, la segunda reconoce un patrón específico de ataque en un entorno observado; ambas capacidades se basan en un motor robusto y rápido que puede detectar patrones complejos tan rápido como sea posible [7]. Entonces se podría afirmar que un Honeypot es un IDS, por ser un sistema capaz de detectar cualquier tipo de intruso o de vulnerabilidad presente en las redes de datos y sistema informático.

### **Honeypots y Honeynets**

#### **Honeypot**

La conceptualización del tema Honeypot proviene de varios estudios en el área de Seguridad las redes de computadoras. El trabajo de los administradores de red, consiste en mantener todos los servicios y sistemas funcionales. Si los administradores examinaran periódicamente la red, podrían detectar un alto nivel de intrusiones de acceso ajeno al

sistema o servicio, la detección de una vulnerabilidad en el sistema no tiene por qué implicar un fallo del mismo, los ciberataques y amenazas persistentes avanzadas requiere un nuevo enfoque de protección y prevención, al descubrir a un atacante en potencia, permitirá tomar las medidas necesarias y oportunas antes de que entre al sistema real o servicio en ejecución. Cada uno de los sistema trampa no puede ser utilizado para fijar cualquier servicio, incluso peor, un Honeypot puede atraer más interés en una red específica que se requiera, Ver Gráfico 2.2. 1.

Un Honeypot es utilizado para ayudar evitar riesgos o delitos informáticos en una organización, asume la intención de reunir la mayor cantidad de información posible, estos Honeypots agregan niveles de seguridad de una organización, pero pueden ayudar a entender a la comunidad blackhat y sus ataques, así como para construir algunas defensas contra las amenazas de seguridad informática [8].

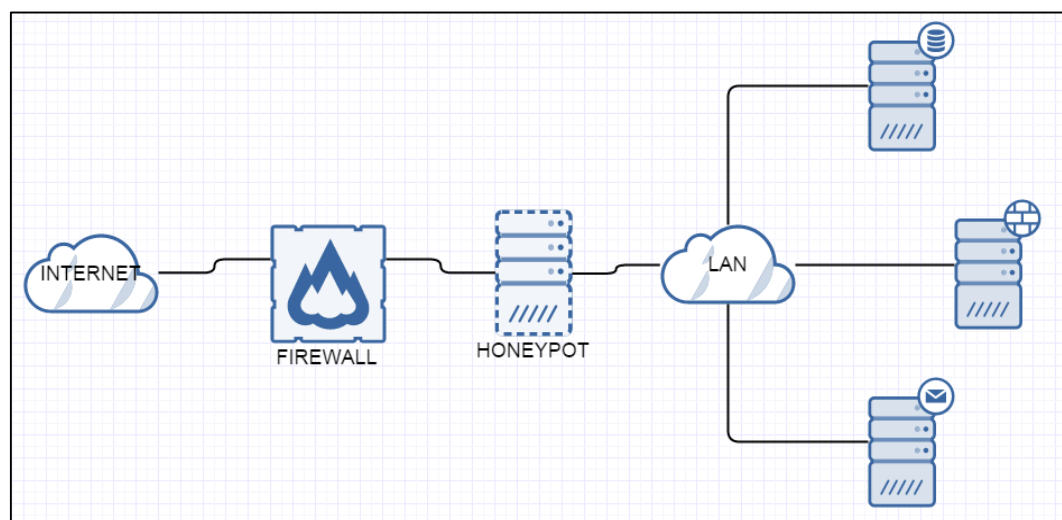


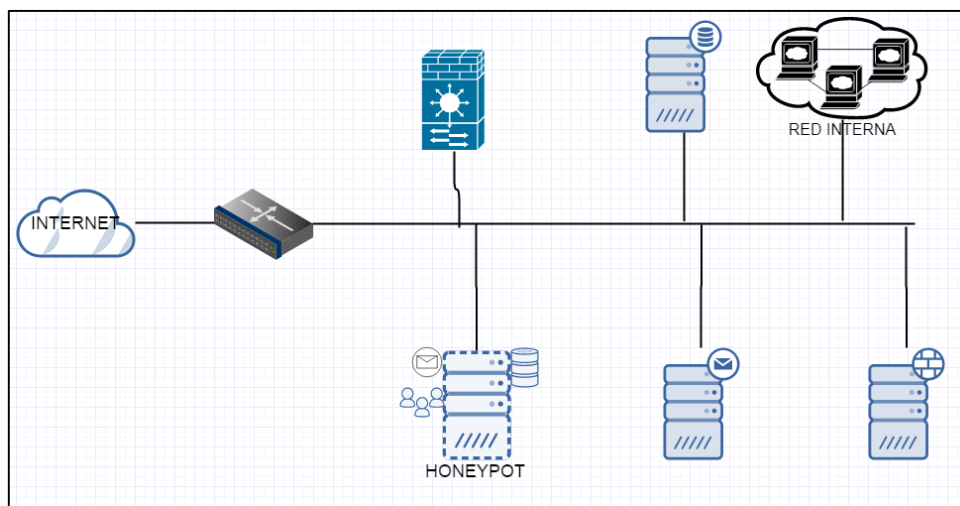
Gráfico 2.2. 1 Honeypot diagrama general.

Elaborado por: Javier Vargas

## Honeypot en la red

Cada tráfico desde y hacia un Honeypot es sospechoso, en general es una actividad no autorizada. Por consiguiente, todos los datos recogidos por un Honeypot son datos desordenados en primera instancia, para después ser tabulados, donde en general no se

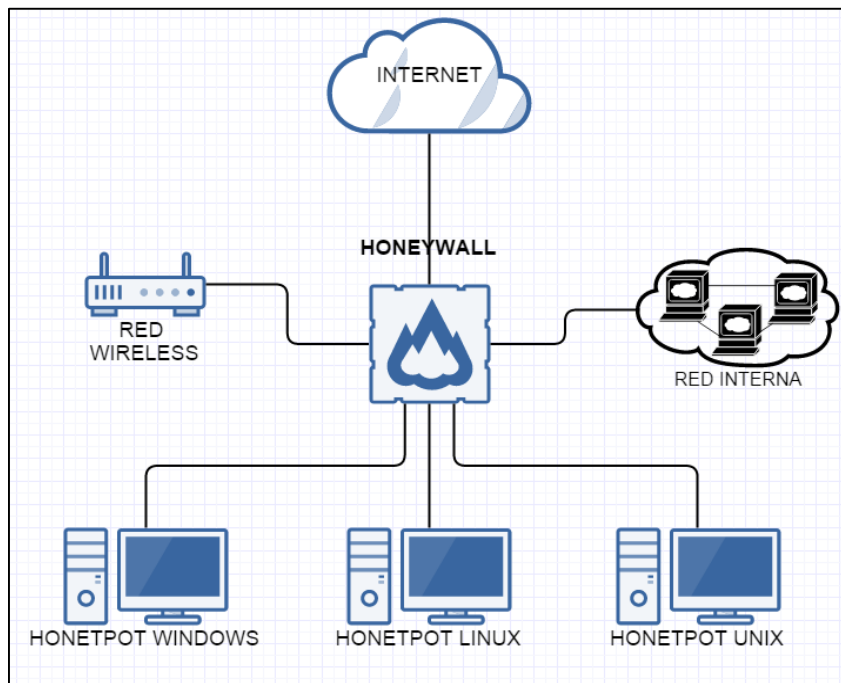
produce una gran cantidad de registros porque los sistemas se están ejecutando en esa máquina [9], ver Gráfico 2.2. 2. El análisis de estos datos debería ser mucho más fácil ya que los datos recogidos por un Honeypot son de gran valor y pueden conducir a una mejor comprensión y conocimiento que a su vez puede ayudar a aumentar la seguridad de la red.



**Gráfico 2.2. 2 Honeypot como equipo físico en la red**  
Elaborado por: Javier Vargas

## Honeynet

Existen configuraciones de Honeypots simples, estos se ejecutan en una sola máquina para hacer que los Honeypots se reflejen en los sistemas anfitriones, los usuarios administradores manejan sistemas complejos de configuración que constan de múltiples Honeypots, IDS y componentes de cortafuegos [10], ver Gráfico 2.2.3, estas configuraciones complejas se denominan redes trampa.



**Gráfico 2.2. 3 Diagrama Honeynet**  
**Elaborado por: Javier Vargas**

Además las redes Honeynets permiten la simulación de entornos productivos reales a costa de un mayor o menor inmenso gasto administrativo y técnico, los archivos de registro de las redes trampa, por ejemplo, son mucho más difíciles de interpretar en comparación con la salida de un solo Honeypot. Pueden ocurrir situaciones extraordinarias, donde son atacados y mal utilizados por diversos componentes de terceros. Existen Honeypots gratuitos y comerciales disponibles en el mercado, su funcionalidad difiere en gran medida, así como su complejidad y facilidad de uso [11].

### **Riegos o inseguridades informáticas más comunes**

Los efectos van desde bajo involucramiento de Honeypots de alta participación de riesgo, la protección, prevención, detección y respuesta a los ataques de baja interacción en sistemas de producción, ver Gráfico 2.2. 4, facilitan la recolección de la información, esto ayuda a definir tendencias respecto de las actividades del atacante, activación de sistemas tempranos de alarma, predicción de ataques e investigaciones con alta interacción [12]. El

uso de redes trampa están disponibles, teniendo en cuenta el alto riesgo, los conocimientos necesarios para gestionar un sistema de este tipo y el hecho de que todavía hay muchas incertidumbres, la investigación en curso sobre este tema es una gran sorpresa. La evaluación de riesgos maneja un esquema estructurado, apuntado todos los análisis a las vulnerabilidades que se puedan encontrar en sistema de información o red de datos.



Gráfico 2.2. 4 Modelo evaluación de riesgos

Fuente: <https://seguridadinformaticaufps.wikispaces.com/file/view/8.JPG/329075810/531x342/8.JPG>

## Tipos de Honeypot.

### Honeypots de baja interacción

#### Specter

“Intrusion Detection System”, un Honeypot fundamentado en sistemas de detección de intrusos, sensibles para a los atacantes, este sistema suministra servicios web y servicios de correo, que atraen cómodamente a los atacantes, pero en contexto son trampas que pretenden recoger información [11].

### Honeyd

Un Honeypot que establece host virtuales en la red, estos sistemas pueden ser configurados para establecer servicios parciales y su naturaleza puede ser adaptada de modo que parezcan estar estableciendo sistemas operativos. Honeyd incrementa la seguridad de autocontrol proporcionando mecanismos para la detección y evaluación de vulnerabilidades [11].

### KFSensor

Honeypot de Windows, un sistema de detección de intrusos (IDS) que actúa para atraer y detectar piratas informáticos y gusanos de red, además detecta sistemas vulnerables mediante la situación de los servicios del sistema y troyanos.

### PatriotBox

Usa como señuelo el sistema de detección de intrusos (IDS), los medios de red empresarial de forma segura a la detección temprana de las amenazas de intrusos. También maneja asistencia para reducir el spam en Internet ya que aparenta un Servidor de correo de retransmisión directa [11].

## **Honeypots de Alta interacción.**

### HoneyNet

Es un tipo de Honeypot de alta interacción y está diseñado para recopilar un alto grado de información sobre las amenazas comprometidas en la organización, la Honeynet suministra un medio real de los sistemas, aplicaciones y servicios para atender con los atacantes, siendo una Honeynet un conjunto o grupo de Honeypots [13] .

### ManTrap

Puede crear un “software jaula” capaz de simular una red virtual de una máquina. Para ello emula una variedad de servicios en una sola ManTrap. Este Honeypot es configurable para

notificar al administrador, de posibles alertas que puede enviar correo a cualquier dirección e-mail o un dispositivo con contenido SNMP, alertando que han entrado a la “jaula” [13].

### HoneyWall

El Honeywall CDROM es un CD que posee herramientas necesarias para configurar una Honeynet (red trampa) de segunda generación. El CDROM está basado en una versión reducida de Linux y está diseñado para ser utilizado como aplicación: contiene sólo las herramientas que son necesarias para controlar el Honeywall, ver Gráfico 2.2. 5.

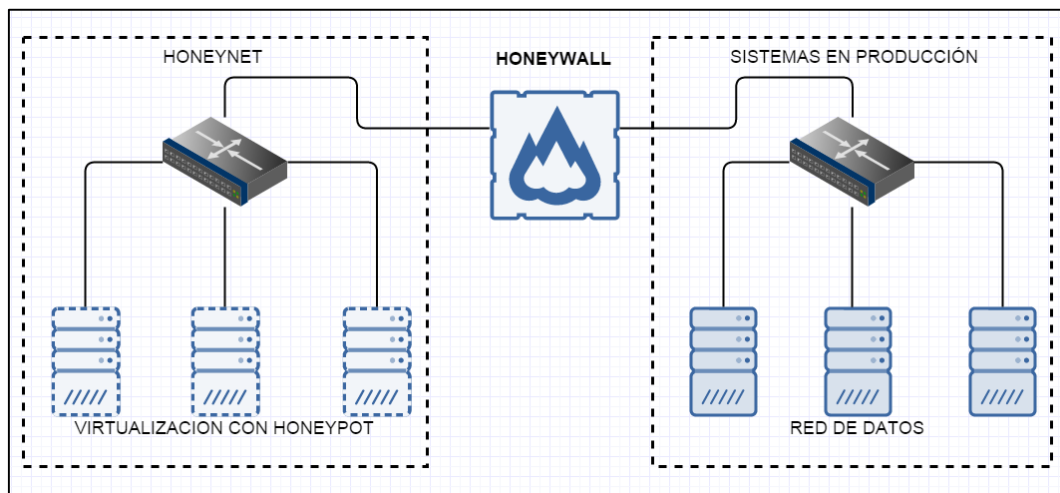


Gráfico 2.2. 5 HoneyWall

Elaborado por: Javier Vargas

### **Procedimiento de captura y análisis**

ManTrap emplea un sniffer de red para recoger todos los paquetes de red dirigidas hacia o desde el host ManTrap [14]. El módulo de reglamentarias registra toda la lectura o escritura de información durante una sesión de terminal, ver Gráfico 2.2. 6.

```
192.168.1.96 68.177.102.20 / 0.170081
192.168.1.96 68.177.102.20 /stylesheets/smoothness-css 0.170682
192.168.1.96 68.177.102.20 /scripts/jquery 0.173387
192.168.1.96 68.177.102.20 /scripts/jquery-highlight 0.172521
192.168.1.96 68.177.102.20 /scripts/cookie_reader 0.175224
192.168.1.96 68.177.102.20 /scripts/snort 0.170195
192.168.1.96 68.177.102.20 /scripts/jquery-ui 0.173404
192.168.1.96 68.177.102.20 /scripts/rule-search 0.169380
192.168.1.96 68.177.102.20 /stylesheets/screen-css 0.164117
192.168.1.96 209.85.227.113 /ga.js 0.097584
```

Gráfico 2.2. 6 Análisis del atacante en la red (Kali Linux)

Elaborado por: Javier Vargas

### Información recolectada

La minería de datos, es un método para ver los datos en tiempo real y otra para inspeccionar miles de alertas sin conexión. Un conjunto de herramientas de minería de datos es muy útil e importante en un IDS para utilizar todo su potencial [15]. Otras cualidades importantes para los sistemas de detección de intrusiones son " bajas tasas de falsas alarmas".

### 2.3 Propuesta de Solución

En la Implantación de un Honeypot como herramienta de prevención y detección de intrusos, facilitará la gestión administrativa en el área de redes, la gestión de la información y fácil control en procesos operativos cotidianos de seguridad informática, permitiendo obtener datos reales en donde la información será presentada, tabulada con respecto a las vulnerabilidades de servicios que se ejecutan en un sistema determinado y los ataques que reciben las redes de datos de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato.



# **CAPÍTULO 3**

## **METODOLOGÍA**

### **3.1 Modalidad de la investigación**

La presente investigación se contextualiza en la modalidad de investigación documental y de campo, dado que se van a aplicar conocimientos científicos nuevos, limitando al área de investigación en la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, apoyándose de los fundamentos y políticas permitidos sobre seguridad informática, por lo cual el análisis con lleva una herramienta de investigación forense.

### **3.2 Recolección de información**

Para la recolección de la información sobre el análisis de la red de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la ciudad de Ambato, se determina el uso de Internet y la guía del tutor para el análisis de la parte técnica, en donde las Honeynets no son un producto, son toda un arquitectura, una red con un ambiente totalmente controlado.

### **3.3 Procesamiento y análisis de datos**

Las técnicas de análisis de datos se refieren a los procedimientos o formas particulares de obtener los datos o información necesaria para llevar a cabo la investigación.

- Control de datos.
- Procesamiento de datos.
- Captura de datos.
- Análisis de los datos.
- Exclusión de inconsistencia de la información.
- Interpretación de los datos.

- Cuadros de presentación de la información recolectada.

### **3.4 Desarrollo del proyecto**

- Analizar las herramientas de detección de intrusos actualmente utilizadas en la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.
- Determinar las políticas y herramientas aplicables en la identificación de vulnerabilidades.
  - El manejo de escenarios controlados.
  - Honeypot para reforzar la seguridad a niveles de aplicación.
  - Honeynet virtuales como medio de transmisión.
  - Gestión de la información.
  - Control de acceso.
- Elaborar el diseño preliminar de una Honeynet.
  - Estudio de las arquitecturas que se generará.
  - Diseño de la red llamada Honeynet.
  - Disposición del equipamiento físico y virtual.
- Documentar los procesos y herramientas usados en la implantación de la Honeynet. Dependiendo del estudio del diseño de la red, se establecerá el equipamiento necesario.
  - Equipamiento necesario.
  - Uso de Software/Hardware.
  - Sistemas Operativos usados.
  - Herramientas de análisis de seguridad informática.

- Escenarios controlados de ciberataques.
- Maqueta de pruebas.
  
- Presentar el análisis realizado por la herramienta Honeypot en la FISEI.
  - La presentación de los resúmenes o logs generados, serán puestas en conocimiento, en presentación claro y fiable para su uso como medio de prevención.
  - Presentación de documentación final.

## CAPÍTULO 4

### DESARROLLO DE LA PROPUESTA

El proyecto de grado comprende sobre la tecnología de Honeypots, teniendo en cuenta que el análisis como un proceso sistemático para estimar la magnitud de amenazas y vulnerabilidades informáticas existentes en la FISEI, es así que por cada objetivo específico se realizan pasos concretos como se detallan a continuación:

#### 4.1 Análisis

Para el análisis se establece una Entrevista no estructurada con un máximo de dos preguntas realizadas por autor Javier Vargas, establecidas directamente con el Ingeniero Eduardo Chaso administrador del Departamento de Redes.

- Preguntas no estructuradas:

¿Existe algún mecanismo de seguridad informática?

*La facultad no cuenta con un sistema de seguridad informática para la protección de los datos e información, ya que no son muy importantes para usuarios ajenos a la facultad. Actualmente se maneja la seguridad informática por las configuraciones de los Servidores y Routers, creando así VLANs que separa lo Administrativo de lo Académico.*

¿Es factible la implementación de un sistema de prevención y detección de intrusos?

*Factible como medio de investigación, puede ser muy útil para prevenir algún tipo de acceso no autorizado, ya que la parte administrativa tiene en sus computadores información valiosa, como facultad si debemos tener un sistema de seguridad informática no demasiado complejo pero que sea estable y seguro.*

Una vez terminada la entrevista se puede afirmar que la FISEI no dispone actualmente de mecanismos de prevención y de mecanismos de protección de los datos integrados en sus redes. Pero se contempla las configuraciones de los Servidores y Routers como medio de seguridad en la red de datos.

La factibilidad de implementar un sistema de prevención y detección de intrusos es contemplado en la entrevista como medio de investigación. Entonces se establece un análisis de la infraestructura informática de la facultad, analizando los dispositivos que se puedan encontrar, sus configuraciones y funciones dentro de la red de datos.

### **Identificación de Equipos o Sistemas de Seguridad en la red de datos de la FISEI**

En la facultad cuenta con tres Servidores actualmente en funcionamiento, los cuales son:

#### **Servidor de Aplicaciones.**

- Configuración del Firewall: permitir la conexión, permitir una conexión solo si está protegida mediante el uso de protocolo de seguridad de Internet (IPsec) o bloquear la conexión.
- Parches para software: son programas que permiten modificar o hacer cambios a una aplicación para corregir errores, alterarla su funcionamiento o para hacer actualizados.
- Licencias: se establece las retribuciones del propietario al usuario finito en una o varias copias del programa informático, existiendo dos tipos de licencias; Software propietario (reserva de derechos sobre el uso, modificación o redistribución del software) y open source (permitiendo que tanto el código fuente puedan ser modificados y redistribuidos libremente).

#### **Servidor Proxy.**

- Uso de registros o “Logs”: un registro de actividad de un sistema que permite que el administrador pueda determinar las políticas de seguridad de la red de datos y en el sistema como tal.

- Niveles de acceso: el acceso al Servidor o a la red de datos, es configurado por el Protocolo AAA; autenticación, autorización y contabilización (en inglés, Authentication, Authorization and Accounting), además por las políticas de seguridad establecidas en la organización, institución o empresa.
- Reglas ACL: reglas de control de acceso que establecen políticas centralizadas para una mejor y efectiva administración de la red.

### **Servidor de Enrutamiento.**

Configuración VPN (Red privada virtual):

- Establece comunicaciones seguras de acceso proporcionados para usuarios característicos.
- Mejora el alcance de las redes, para establece parámetros de conexión entre varias subredes y accesos a las mismas.
- Las redes privadas virtualizadas proporcionan un mayor nivel permisible de seguridad mediante seguridad IP (IPsec) o túneles VPN de Secure Sockets Layer (SSL) y tecnologías de autenticación.

### **Funciones de los Servidores**

Servicios instalados en un Servidor.

- Los registros del sistema operativo (sobre todo en materia de seguridad y los registros de sucesos).
- Configuración de la red (incluyendo colocación lógica de la red del Sistema Honeypot).
- Aplicaciones instaladas (y sus respectivos parámetros y funciones)
- Los usuarios y grupos de usuarios (incluyendo miembros del grupo y de las capacidades).
- "dummy" información dentro del Servidor (y su naturaleza).

La identificación de dichos equipos tiene como funcionalidad describir la red, lo cual va a servir como plataforma para la ubicación del Honeypot en la Honeynet que se va implantar. La Facultad de Ingeniería en Sistemas, Electrónica e Industrial, cuenta con un Departamento de Redes, encargado principalmente del mantenimiento y gestión Informática y Tecnológico de la Facultad, en este proyecto de investigación se implementa una red Honeynet Virtual.

## **4.2 Determinar las políticas y herramientas aplicables**

### **Políticas de Seguridad Informática de la FISEI en la Administración de Redes**

*"Cuando no ocurre nada, nos quejamos de lo mucho que gastamos en seguridad. Cuando algo sucede, nos lamentamos de no haber invertido más... Más vale dedicar recursos a la seguridad que convertirse en una estadística." Autor: Anónimo.*

El administrador de red establece ciertas políticas de seguridad informática, las cuales van regidas a los estándares y reglas que se configuran en los equipos Informáticos, ver Gráfico 4.2. 1, para la protección de la información y mantener siempre un servicio activo. Una serie de mecanismos de seguridad son constituidos por varias herramientas para la protección del sistema o servicio, entre ellos se encuentra la definición de un Honeypot, los mecanismos de seguridad se establecen en tres grupos:

- **Prevención:** control de acceso con respecto a la política de seguridad establecida.
- **Detección:** aislamiento de los intentos de intrusión y acceso no autorizado.
- **Recuperación:** uso de las copias de seguridad o Backups del sistema para recuperar su normal funcionamiento.

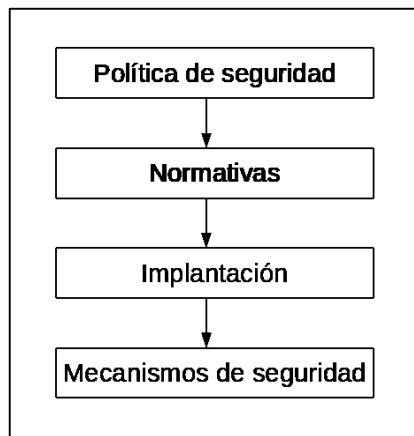


Gráfico 4.2. 1 Políticas de Seguridad

Elaborado por: Javier Vargas

### **Niveles de Seguridad Informática**

El estándar de niveles de seguridad más utilizado internacionalmente es el TCSEC Orange Book, desarrollado en 1983 de acuerdo a las normas de seguridad en computadoras del Departamento de Defensa de los Estados Unidos [16].

#### **Nivel D:**

Este nivel contiene sólo una división y está reservada para sistemas que han sido evaluados y no cumplen con ninguna especificación de seguridad. Sin sistemas no confiables, no hay protección para el hardware, el sistema operativo es inestable y no hay autenticación con respecto a los usuarios y sus derechos en el acceso a la información.

#### **Nivel C1:**

Se requiere identificación de usuarios que permite el acceso a distinta información. Cada usuario puede manejar su información privada y se hace la distinción entre los usuarios y el administrador del sistema, quien tiene control total de acceso.

#### **Nivel C2: Protección de Acceso Controlado**

Este subnivel fue diseñado para solucionar las debilidades del C1. Cuenta con características adicionales que crean un ambiente de acceso controlado. Se debe llevar una



auditoria de accesos e intentos fallidos de acceso a objetos. Tiene la capacidad de restringir aún más el que los usuarios ejecuten ciertos comandos o tengan acceso a ciertos archivos, permitir o denegar datos a usuarios en concreto, con base no sólo en los permisos, sino también en los niveles de autorización.

### **Nivel B1: Seguridad Etiquetada**

Este subnivel, es el primero de los tres con que cuenta el nivel B. Soporta seguridad MULTINIVEL, como la secreta y ultra secreta. Se establece que el dueño del archivo no puede modificar los permisos de un objeto que está bajo control de acceso obligatorio.

Cada usuario que accede a un objeto debe poseer un permiso expreso para hacerlo y viceversa. Es decir que cada usuario tiene sus objetos asociados.

También se establecen controles para limitar la propagación de derecho de accesos a los distintos objetos.

### **Nivel B2: Protección Estructurada**

Requiere que se etiquete cada objeto de nivel superior por ser padre de un objeto inferior.

La Protección Estructurada es la primera que empieza a referirse al problema de un objeto a un nivel más elevado de seguridad en comunicación con otro objeto a un nivel inferior.

El sistema es capaz de alertar a los usuarios si sus condiciones de accesibilidad y seguridad son modificadas; y el administrador es el encargado de fijar los canales de almacenamiento y ancho de banda a utilizar por los demás usuarios.

### **Nivel B3: Dominios de Seguridad**

Refuerza a los dominios con la instalación de hardware: por ejemplo el hardware de administración de memoria se usa para proteger el dominio de seguridad de acceso no autorizado a la modificación de objetos de diferentes dominios de seguridad. Además, cada usuario tiene asignado los lugares y objetos a los que puede acceder.

### **Nivel A: Protección Verificada**

Es el nivel más elevado, incluye un proceso de diseño, control y verificación, mediante métodos formales (matemáticos) para asegurar todos los procesos que realiza un usuario sobre el sistema. Para llegar a este nivel de seguridad, todos los componentes de los niveles inferiores deben incluirse. El diseño requiere ser verificado de forma matemática y también se deben realizar análisis de canales encubiertos y de distribución confiable. El software y el hardware son protegidos para evitar infiltraciones ante traslados o movimientos del equipamiento. Los niveles de Seguridad Informática ayudan a establecer políticas de acceso y poder crear o modificar las reglas negociadas entre los clientes hacia Servidor y viceversa, además las conexiones permitidas por los Routers de configuración por VLANs.

### **Herramientas aplicables en las tecnologías Honeypots**

En esta etapa se describe el tipo de Honeypot según su arquitectura de red de la FISEI para el proyecto de investigación, igualmente se exponen las razones por que fueron seleccionadas para los distintos análisis, ver Tabla 4.2. 1.

<b>Honeypot</b>	<b>Nivel</b>	<b>Características</b>	<b>Factibilidad para el proyecto de investigación</b>	<b>Código abierto o Código propietario</b>
<b><u>Honeyd</u></b>	Baja Interacción	Crea hosts(maquinas) virtuales en una red, se lo puede configurar para ejecutar servicios arbitrarios, además son completamente adaptables a cualquier SO(sistema operativo)	El uso de este tipo de Honeypot pretende acoplar a una red muy sencilla su sistema de prevención y detección de intrusos, dependiendo de los servicios que preste la red de datos de la FISEI.	Honeyd es un software de código abierto publicado bajo Licencia Pública General GNU

<b><u>HoneyNet</u></b>	Alta Interacción	HoneyNet es diferente de los HoneyPots comunes, es lo que clasificaríamos como un HoneyPot para la investigación, su principal funcionalidad es recoger información de las amenazas no de los atacantes como tal.	Muy sencillo en la práctica pero muy eficiente en su análisis, dependiendo de los servicios, lo que lo convierte en un HoneyPot de producción. Factible para la seguridad de la información, siendo una herramienta de fácil acceso y manejo.	Licencia Libre de Documentación GNU, versión 1.2 o cualquier versión posterior publicada por la Free Software Foundation (Fundación para el Software Libre)
<b>HoneyWall</b>	Alta Interacción	HoneyWall CDROM, su configuración crea una plataforma para tecnologías más especializadas, su principal funcionalidad es en temas forenses (captura y análisis).	Factible por la escalabilidad del HoneyPot existen tres puntos importantes que beneficiarían al proyecto de investigación: Defensa de la red. Análisis forense en tiempo real. Monitorización de tráfico.	Licencia de Documentación Libre GNU (FDL), versión 1.2 o cualquier versión posterior publicada por la Free Software Foundation.

**Tabla 4.2. 1 HoneyPots experimentales**

**Elaborado por: Javier Vargas**

## Funcionalidad a niveles de aplicación

La virtualización de un Honeypot obedece a su funcionalidad para la cual se implementara, por ejemplo para nuestro caso se ha seleccionado un Honeypot de Alta interacción, el cual proporcionara mayor información de riesgo sobre los datos obtenidos por intrusos además información sobre el atacante en cuestión, ver Gráfico 4.2. 2.

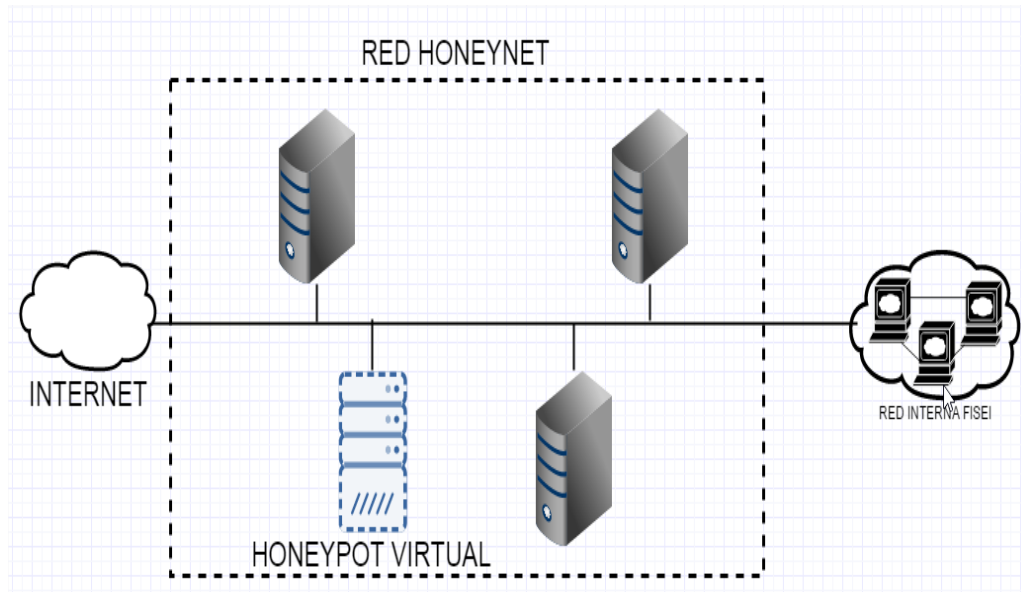


Gráfico 4.2. 2 Modelo red de datos de la FISEI -  
Elaborado por: Javier Vargas

## Escenarios Controlados para normas de seguridad informática.

Los problemas de seguridad relacionados a cualquier tipo de servicio pueden ser controlado por reglas de Firewall, pero cuando se produce un ciberataque la principal vulnerabilidad que buscan es encontrar el puerto y servicio más vulnerable, a continuación se describen determinados puertos de determinados Servidores (WINDOWS SERVER y CENTOS) Tabla 4.2. 2:

PUERTO	SERVICIO	PROTOCOLO	DESCRIPCIÓN
21	FTP	TCP/UPD	Protocolo de transferencia de archivos.
22	SSH	TCP/UPD	Protocolo para comunicaciones seguras.
23	TELNET	TCP/UPD	Permite la conexión con terminales y aplicaciones
25	SMTP	TCP/UPD	Protocolo de transferencia simple de correo.
53	DNS	TCP/UPD	Protocolo o servicio de nombres de dominio.
69	TFTP	TCP/UPD	Protocolo de transferencia de archivos trivial.
80	HTTP	TCP/UPD	Protocolo para la transferencia de hipertexto.
137	NETBIOS-NS	TCP/UPD	Interfaz para acceso a servicios de red (NOMBRE DEL SERVICIO).
139	NETBIOS-SSN	TCP/UPD	Interfaz para acceso a servicios de red (SESIÓN DEL SERVICIO).
143	IMAP	TCP/UPD	Protocolo de acceso a mensajería en el Internet.
220	IMAP3	TCP/UPD	Protocolo seguro de IMAP.
389	LDAP	TCP/UPD	Protocolo de acceso a directorios.
443	HTTPS	TCP/UPD/SCTP	Protocolo seguro de HTTP
3128	SQUID	TCP/UPD	Servidor proxy para web con cache.
3306	MYSQL	TCP/UPD	Servicio de gestión de base de datos.
8080	WEBCACHE	TCP/UPD	Optimizado para el Protocolo HTTP
5432	POSTGRES	TCP/UPD	Servicio de gestión de base de datos.
1433	SQL SERVER	TCP/UPD	Servicio de gestión de base de datos.

**Tabla 4.2. 2 Puertos y Protocolos**

**Elaborado por: Javier Vargas**

Desde un punto de vista de seguridad de la red de datos, se enlista los puertos más comunes en caso de un ataque, para desviar la atención de los intrusos se gestiona estos puertos y servicios para que actúen como señuelo en un Honeypot.

### **Honeypot en producción a niveles de aplicación.**

Los aspectos técnicos y operativos, pretenden garantizar el uso e implementación de un Honeypot en producción, se describe un mecanismo que puede ser muy bueno en análisis, pero a su vez también ser muy peligroso dependiendo de la información crítica obtenida, la creación de un Sistema señuelo o trampa, es puesto en ejecución para que la víctima acceda con diferentes técnicas de ataques o perspicacia al momento de vulnerar la seguridad, englobando todos estos aspectos, formulamos las siguientes inquietudes.

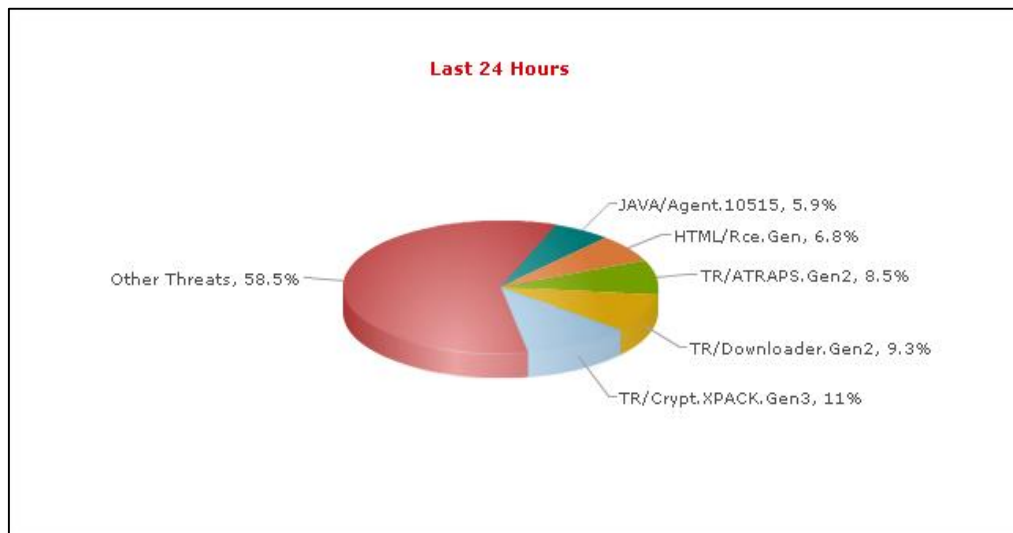
**¿Y si mi Honeypot presenta información relávate a mi Sistema anfitrión?**

**¿Y si mi Honeypot es utilizado como medio de ataque y no de detección?**

**¿Y si el intruso utiliza la información obtenida por el Sistema señuelo para conocer mi infraestructura?**

**¿Y si mi Honeypot es un sistema trampa para q el intruso o atacante acceda al Servidor real?**

Diversas empresas de antivirus de gran gama en servicio de protección, aseguran la efectividad operativa en la implementación de un Honeypot. El sistema de emisión de alertas Avira OASYS (Outbreak Alert System) recopila malware de distintas fuentes. Por esta razón utilizamos distintas tecnologías Honeypot (tarro de miel), servicio instalado en una red, tiene la trabajo de supervisar la red y archivar los ataques.

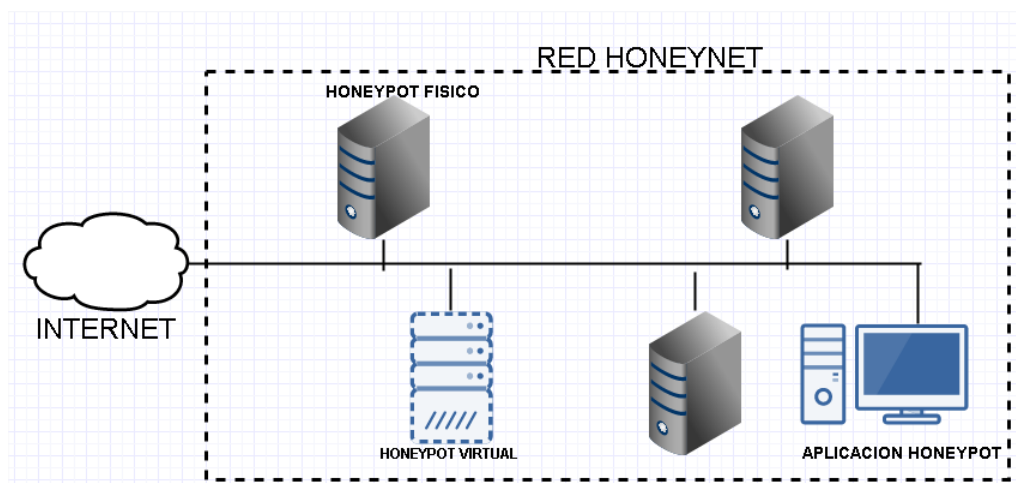


**Gráfico 4.2. 3 Análisis de vulnerabilidades Avira OASYS**

Fuente: <http://www.avira.com/es/support-threats-top-statistics>

Una red de datos con el diseño de una Honeynet gestión la administración más adecuada en el proceso de análisis, como principal configuración el Honeypot de alta interacción Honeywall, representa un mayor nivel de seguridad para la red de datos de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, además como segunda configuración un Honeyd, ya que la información encontrada en la Facultad puede no ser muy relevante.

### Red Honeynet básica



**Gráfico 4.2. 4 Honeynet Básica en una red local**

Elaborado por: Javier Vargas

El esquema de una Honeynet básica tiene dos parámetros de configuración, el primero se establece si el Honeypot es configurado como un Gateway, y el segundo se establece por ser configurado como Servidor o Sistema trampa, para el estudio del proyecto se configura ambas opciones.

### Virtualización de un Honeypot

Una red virtual es configurada en una Honeynet, que actúa como un único computador mediante algún tipo de software de virtualización, permitiendo la ejecución simultánea de varios Sistemas Operativos, creando así recursos del sistema anfitrión simulando la ejecución de los servicios en máquinas diferentes, una Honeynet puede estar establecida por los siguientes parámetros implícitos de configuración:


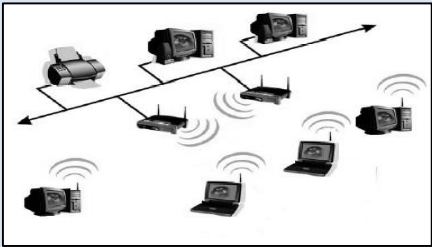
Ubicación	Medio
<p>Red donde se conectara nuestro Servidor o sistema Honeypot, es contemplada por las restricciones previamente estipuladas por el administrador de la red.</p>  <p>Gráfico 4.2. 5 Servidor en la red de datos. Fuente: <a href="http://glosariodeinformatica.com/servidor_de_red_2.jpg">http://glosariodeinformatica.com/servidor_de_red_2.jpg</a></p>	<p>El medio de acceso del atacante será por el medio de comunicación la Internet o por la red local de la facultad, sea esta inalámbrica o cableada.</p>  <p>Gráfico 4.2. 6 Medio de acceso para su control Fuente: <a href="http://1.bp.blogspot.com/-neSli2Vkl9s/s400/red_de_area_local.jpg">http://1.bp.blogspot.com/-neSli2Vkl9s/s400/red_de_area_local.jpg</a></p>

Tabla 4.2. 3 Simplicidad de la red

Elaborado por: Javier Vargas



## Software de virtualización:

VMWare: simular cualquier sistema operativo, los beneficios de virtualización que proporciona son VMWare Player entre otros.

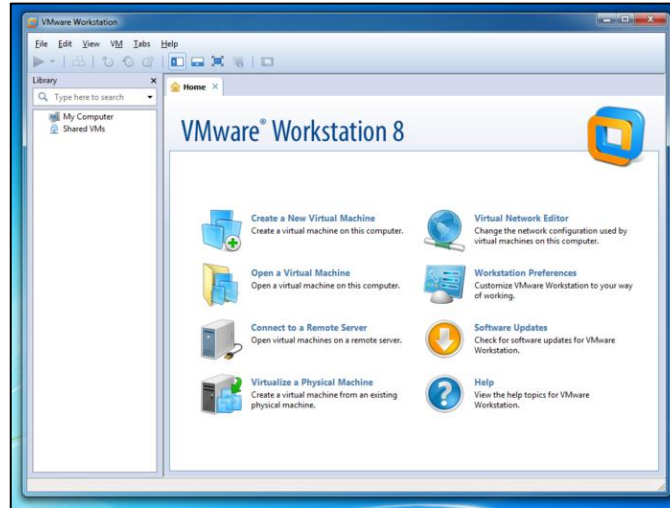


Gráfico 4.2. 7 Software VMWare

Elaborado por: Javier Vargas

VirtualBox: es un proyecto de Sun, gratuito y de código abierto, la ventaja de usar VirtualBox, recae en análisis previos en IDS, un VirtualBox es menos detectable que VMWare, la tecnología de virtualización más robusta entre otras características por las cuales se usa este Software de virtualización.



Gráfico 4.2. 8 Software VirtualBox

Elaborado por: Javier Vargas

Qemu: proyecto de código abierto que puede usarse tanto como emulador virtualizado, disponible solo para entornos Linux.

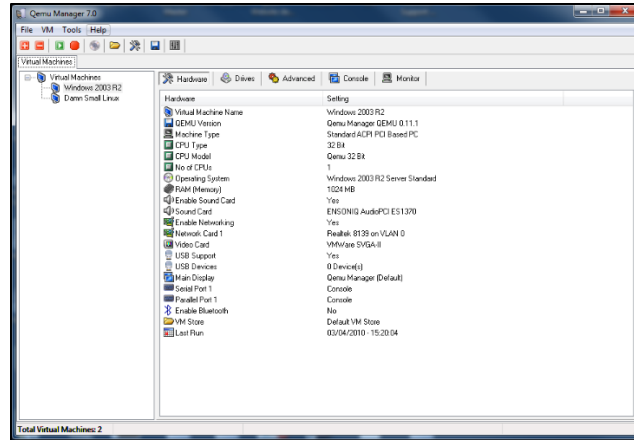


Gráfico 4.2. 9 Software Qemu

Elaborado por: Javier Vargas

User-Mode Linux: es una forma de simular un núcleo de Linux “virtual”, puede simular otro kernel, complejo de configuración pero robusto en Software de virtualización.

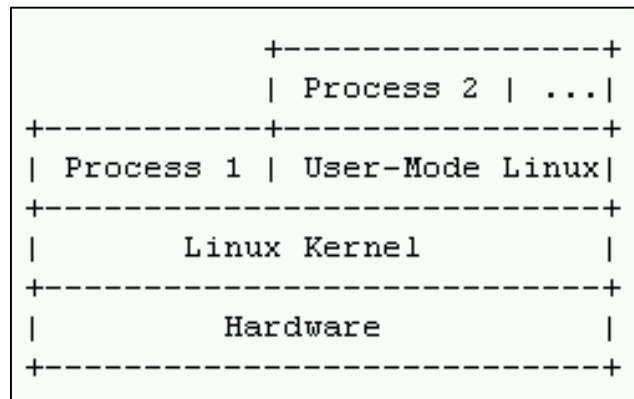


Gráfico 4.2. 10 Modulo User-Mode Linux

Elaborado por: Javier Vargas

La solución libre de VirtualBox puede cubrir de sobra las necesidades de virtualización, desde un nivel de seguridad informática, además como software de virtualización para arquitecturas X86/amd64 de Oracle, funciona en Linux, Mac, Solaris y Windows, otorgando soporte para IPv6, conexiones virtuales RDP (opción Adaptador sólo-anfitrión),

sobre el código virtual de VT-x y AMD-V con corrección de errores y mejora de rendimiento. Para el proyecto de investigación se optó por VirtualBox.

### **Información y Recolección de datos**

La captura de datos obtenida por un Honeypot, puede ser la información más relevante que se tiene de un atacante, el propósito del documento es tener un mejor control para poder alimentar las reglas de seguridad informática en la FISEI, toda la información recolectada debe ser tabulada para ser enviada o analizada únicamente por el administrador de red, existiendo un medio seguro para su almacenamiento, ya que esto implica que la información es de varios atacantes y puede ser usada para acceder fácilmente o saber cuál son los niveles de seguridad que se encuentran restringidos o controlados.

### **Control de Acceso**

En el espacio de trabajo, todos los equipos se encuentran conectados a un Servidor considerado como un sistema centralizado, la función del administrador de redes de datos de la FISEI, se enfoca a proteger la red contra los desconocidos o atacantes que intentan obtener acceso, debido a este tipo de restricciones se establece los siguientes niveles jerárquicos de seguridad para el proyecto de investigación:

### **4.3 Diseño de una Honeynet**

Para diseñar el Honeypot y la Honeynet, seleccionados en las Herramientas aplicables en las tecnologías Honeypots, su principal interés es en el estudio de la red actual y las arquitecturas óptimas para la instalación y configuración de una Honeynet. La arquitectura que se maneja es Software de código abierto, no implica ningún costo para la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

## Red Honeynet

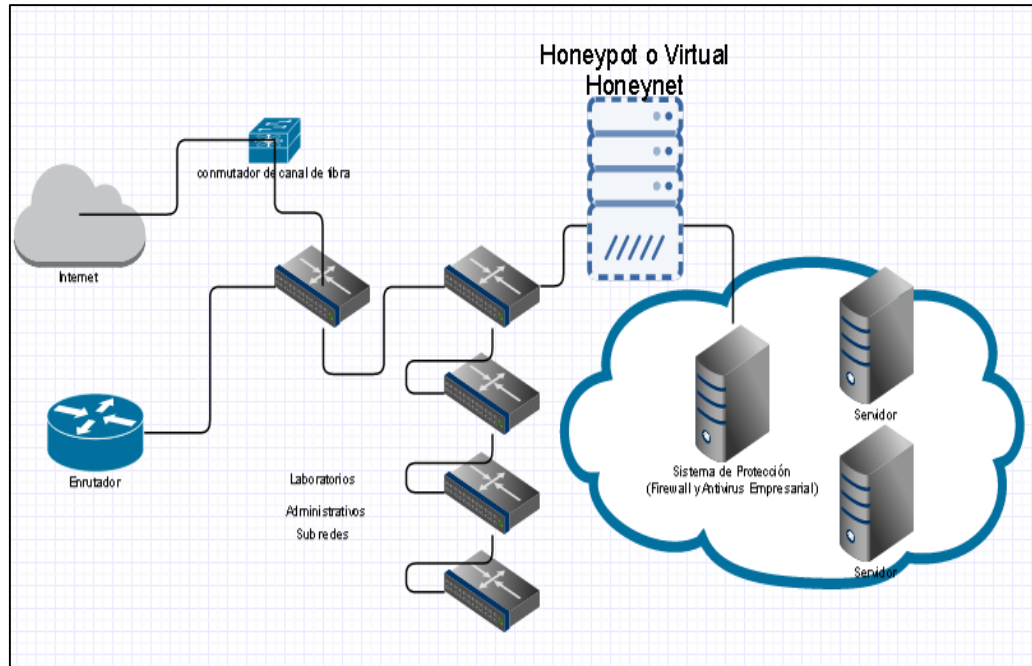


Gráfico 4.3. 1 Red Honeynet Implementada

Elaborado por: Javier Vargas

Esta arquitectura requiere de los siguientes elementos:

- Máquina Virtual
- Red Honeynet
  - Honeywall
  - Honeyd o Sebek.
- Equipos para el monitorio o acceso

## Máquina Virtual

La virtualización del Software que utiliza VirtualBox, es de código abierto bajo los términos de la Licencia Pública General de GNU (GPL) versión 2.

## **Honeywall**

Honeywall CDROM, es un CD-ROM de arranque que instala todas las herramientas necesarias para analizar una red trampa.

### **Resumen Técnico**

- **Funcionamiento**

Honeywall CDROM instala y configura un Gateway como Honeypot, en el disco duro local, mediante un Disco Compacto de Memoria de Sólo Lectura (CD-ROM), donde la información de instalación es eliminada una vez concluida, el núcleo del Honeywall está basado en Fedora Core 6, con el entorno de trabajo por defecto GNOME Shell, su funcionamiento es la captura, análisis de todo el tráfico entrante y saliente a los Honeypot.

La instalación como arranque desde el CDROM, es un proceso completamente robusto y automatizado, con las configuraciones básicas de red, al configurar el Gateway de un Honeywall, se establece por primera vez las tarjetas de red. Existen tres opciones para la administración del sistema:

- Interfaz del navegador GUI.
- Línea de comandos.
- Menú de diálogos.

- **Características**

Honeywall se puede configurar para actualizarse automáticamente, estableciendo los días o periódicamente, esto se usa mediante el comando “yum”, que es un paquete administrador de software, buscando el sistema operativo más reciente y las RPM (Red Hat Package Manager) del Honeywall. Las tarjetas de red pueden ser configurada como mínimo 2, una para poder conectarse a la red externa Internet, y

otra tarjeta de red para conectarse a la red interna o red trampa, pero dependiendo del nivel de administración que desea para el Honeywall se le puede configurar otra tarjeta de red.

- Usuarios y privilegios

Honeywall cuenta con su usuario root por defecto, la primer recomendación es cambiar la clave, ya que el sistema viene con una clave por defecto para poder acceder, las contraseñas del Sistema Operativo solo puede ser cambiada iniciando sección en la interfaz web. Los privilegios locales del root no pueden ser modificados ni heredados, solo el administrador root será el único usuario para ingresar al sistema y administrarlo como tal.

### **Requisitos de Hardware**

Los requisitos o requerimientos mínimos para la instalación de Hardware de un Honeywall se estable en disco duro para almacenamiento, CPU para el nivel de procesamiento y memoria dependiente de la maquina anfitrión, estas como principales requerimientos.

Detalle técnico de los requisitos de Hardware:

- Procesador Pentium III, incluido la tecnología AMD y VIA.
- Disco duro 10GB (recomendación).
- Memoria RAM min 512MB; la memoria depende funcionalmente de la utilidad del Honeywall.
- Tarjetas de red (3 tarjetas eth).

### **Honeyd y Sebek**

Honeyd configurado únicamente como un host virtual, adaptándose fácilmente el SO anfitrión, para nuestro caso son herramientas poco utilizadas debido a su inestabilidad en la configuración. Sebek perteneciente a “The Honeynet Project”, es una herramienta de

captura de datos, su principal característica es analizar o capturar las actividades del atacante en un Honeybot, trabaja en la red Honeybot como cliente.

### Instalación y configuración de Honeywall CDROM

El diseño de la red Honeybot (ver Gráfico 4.3. 2), establece un Servidor Honeybot en donde actuaría el Honeywall, como intermediario entre las conexiones salientes y entrantes hacia nuestro Sistema Operativo trampa con tres interfaces de red, además se configura una terminal para la administración por medio de la Interfaz del navegador GUI como se muestra en el gráfico siguiente:

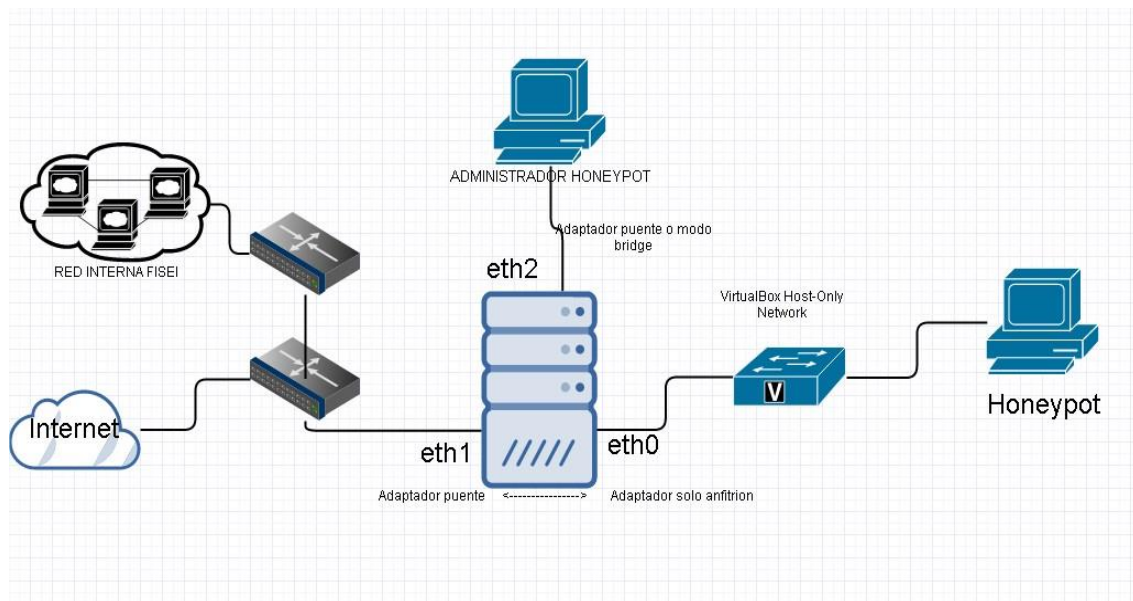


Gráfico 4.3. 2 Honeybot virtual configurado en la red.

Elaborado por: Javier Vargas

**Detalle técnico de las interfaces de red:** La configuración cuenta con tres tarjetas de red “eth”

## eth0: Adaptador solo anfitrión

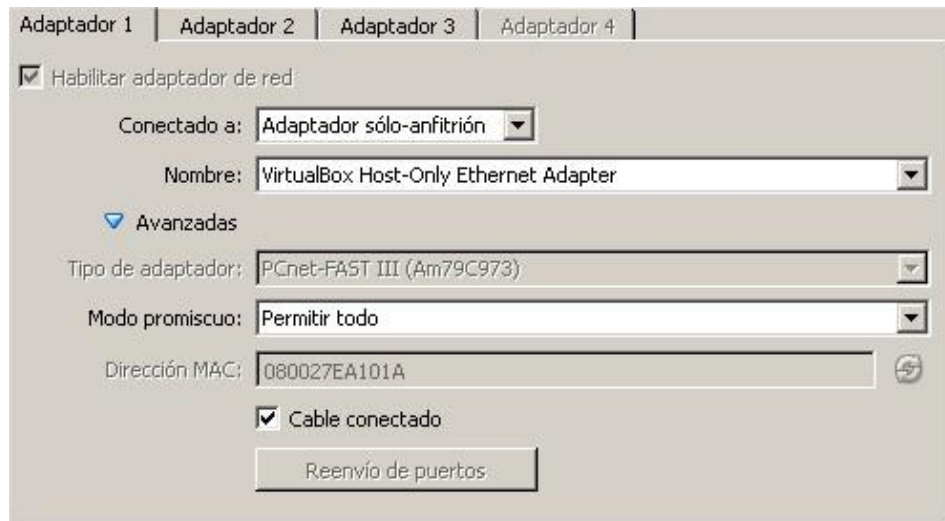


Gráfico 4.3. 3 Adaptador1 de red Honeypot

Elaborado por: Javier Vargas

## eth1: Adaptador puente



Gráfico 4.3. 4 Adaptador2 de red Honeypot

Elaborado por: Javier Vargas



## eth2: Adaptador puente



Gráfico 4.3. 5 Adaptador3 de red HoneyPot

Elaborado por: Javier Vargas

## Direccionamiento lógico IP de la red:

Equipo:	HoneyPot
Dirección IP:	192.168.1.10
Mascara de subred:	255.255.255.0 CIDR /24
Puerta de enlace:	192.168.1.1
Dirección Broadcast:	192.168.1.255
Red IP:	192.168.1.0
SO base:	CentOS
Tarjeta salida:	eth0

Tabla 4.3. 1 HoneyPot configuración de red.

Elaborado por: Javier Vargas

Equipo:	Honeywall Administrador
Dirección IP:	192.168.1.9
Mascara de subred:	255.255.255.0 CIDR /24
Puerta de enlace:	192.168.1.1
SO base:	Linux/Windows
Tarjeta salida:	eth2
Equipo:	Honeywall Salida Internet / Red Local
Dirección IP:	192.168.1.X
Mascara de subred:	255.255.255.0 CIDR /24
Puerta de enlace:	192.168.1.1
SO base:	Linux/Windows
Tarjeta salida:	eth1

**Tabla 4.3. 2 Configuración administrador Honeywall.**

**Elaborado por: Javier Vargas**

Para la Instalación del Honeywall, se puede descargar de la página oficial <https://projects.honeynet.org/honeywall/>, actualmente se encuentra en la versión <<roo-1.4.hw-20090425114542.iso >>. Instalación y configuración más detallada ver **Anexo A1**. La administración puede ser determinada por línea de comandos, menú de diálogos y por interfaz del navegador, cada configuración realizada es reflejada en los tres tipos de gestión.

### **Línea de comandos**

Linux en sus primeras versiones maneja todo tipo de administración por medio de comandos, órdenes o bash (interpretador de órdenes) de configuración. La configuración establecida en el **Anexo A1**, se encuentra en la raíz “/” y la carpeta “etc”, con el nombre honeywall.conf, para la modificación de este archivo se realiza mediante el uso de algún editor de texto instalado en el Sistema o el uso de ordenes enviados por la terminal con el

uso del comando de ejecución HWCTL, permitiendo la configuración de las variables de archivo:

```
[root@localhost etc]# hwctl -r HwALERT=no
```

Contenido del archivo de configuración, los parámetros configurados se encuentran en resaltado:

```
#
#####
#
# Copyright (C) <2005> <The Honeynet Project>
#
# This program is free software; you can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation; either version 2 of the License, or (at
# your option) any later version.
#
# This program is distributed in the hope that it will be useful, but
# WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU
# General Public License for more details.
#
# You should have received a copy of the GNU General Public License
# along with this program; if not, write to the Free Software
# Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307
# USA
#
#####

#
# This file is the Honeywall import file (aka "honeywall.conf").
# It is a list of VARIABLE=VALUE tuples (including comments as
# necessary, # such as this) and whitespace lines.
#
#
#####

#####
# Las variables de sitio que son global a todo el honeywalls #
#####

# Especifica la dirección (es) IP y/o redes que permiten unir al interfaz de dirección
# [Valid argument: IP address(es) | IP network(s) in CIDR notation | any]
HwMANAGER=any

# Especifica el puerto que sobre el cual SSHD escuchará
# [Valid argument: TCP (port 0 - 65535)]
HwSSHD_PORT=22

# Especifica si realmente la raíz puede la conexión remotamente sobre SSH
# [Valid argument: yes | no]
HwSSHD_REMOTE_ROOT_LOGIN=no
```

```

# NTP Servidor (es) de tiempo
# [Valid argument: IP address]
HwTIME_SVR=

#####
# Las variables locales que son #
# specific to each      #
# honeywall at a site.  #
#####

# Especifica el sistema hostname
# [Valid argument: string ]
HwHOSTNAME=localhost

# Especifica el sistema DNS el dominio
# [Valid argument: string ]
HwDOMAIN=localdomain

#Comience el Honeywall sobre boot
# [Valid argument: yes | no]
HwHONEYWALL_RUN=yes

# Usar un sistema sin cabeza.
# [Valid argument: yes | no]
HwHEADLESS=no

# La dirección(es) IP pública de este Honeywall
# [Valid argument: IP address | space delimited IP addresses]
HwHPOT_PUBLIC_IP=192.168.1.10

# DNS permiten a servidores Honeypots para comunicarse
# [Valid argument: IP address | space delimited IP addresses]
HwDNS_SVRS=

# Restringir DNS tienen acceso a Honeypot específico o grupo de Honeypots, lista
# [Valid argument: IP address | space delimited IP addresses | blank]
HwDNS_HOST=

# El nombre del interfaz de red que se enfrenta por fuera
# [Valid argument: eth* | br* | ppp*]
HwINET_IFACE=eth0

# El nombre del interfaz de red que se enfrenta internamente
# [Valid argument: eth* | br* | ppp*]
HwLAN_IFACE=eth1

# La IP interna unida a la interfaz que se enfrenta con la internamente
# [Valid argument: IP network in CIDR notation]
HwLAN_IP_RANGE=192.168.1.0/24

# La difusión de IP se dirige para la red interna
# [Valid argument: IP broadcast address]
HwLAN_BCAST_ADDRESS=192.168.1.255

# Permitir QUEUE apoyo para integrarse con Snort-Inline filtración
# [Valid argument: yes | no]
HwQUEUE=yes

```

```

# La unidad de medida para poner límites de conexión outbound
# [Valid argument: second, minute, hour, day, week, month, year]
HwSCALE=hour

# El número de TCP conexiones por unidad de medida (HwScale)
# [Valid argument: integer]
HwTCPRATE=20

# El número de UDP conexiones por unidad de medida (HwSCALE)
# [Valid argument: integer]
HwUDPRATE=20

# El número de ICMP conexiones por unidad de medida (HwSCALE)
# [Valid argument: integer]
HwICMPRATE=50

# El número de otras IPs conexiones por unidad de medida (HwSCALE)
# [Valid argument: integer]
HwOTHERRATE=10

# Permita al SEBEK el colector que entrega la pulsación y archivos a un sistema
# remoto incluso si un atacante sustituye a demonios como sshd
# [Valid argument: yes | no]
HwSEBEK=yes

# Permita el interfaz Walleye de Web.

HwWALLEYE=yes

# Especifica si si hay que drop SEBEK los paquetes o les permiten para ser enviado
# fuera del Honeynet.
# [Valid argument: ACCEPT | DROP]
HwSEBEK_FATE=ACCEPT

# Especifica el SEBEK dirección IP de anfitrión de destino
# [Valid argument: IP address]
HwSEBEK_DST_IP=192.168.1.15

# Especifica el SEBEK destino port
# [Valid argument: port]
HwSEBEK_DST_PORT=1101

# Permitir SEBEK conexión del Cortafuegos Honeywall logs
# [Valid argument: yes | no]
HwSEBEK_LOG=yes

# Especifica si el menú de diálogo debe ser comenzado sobre la conexión TTY1
# [Valid argument: yes | no ]
HwMANAGE_DIALOG=yes

# Especifica si el puerto de dirección debe ser activado sobre el principio o no.
# [Valid argument: yes | no ]
HwMANAGE_STARTUP=yes

# Especifica la interfaz de red para dirección remota. De ser puesto br0, esto va
# asignado MANAGE_IP al interfaz de puente lógico y permiten a su empleo como a
# Interfaz de dirección
# [Valid argument: eth* | br* | ppp* | none]
HwMANAGE_IFACE=eth2

```

```

# IP de dirección Interfaz
# [Valid argument: IP address]
HwMANAGE_IP=192.168.1.9

# Netmask de dirección Interfaz
# [Valid argument: IP netmask]
HwMANAGE_NETMASK=255.255.255.0

# Default Gateway de dirección Interfaz
# [Valid argument: IP address]
HwMANAGE_GATEWAY=192.168.1.1

# DNS Los servidores de dirección Interfaz
# [Valid argument: space delimited IP addresses]
HwMANAGE_DNS=192.168.1.1

# TCP ports permitido en el interfaz de dirección.
# Do NOT SSHD port
# [Valid argument: space delimited list of TCP ports]
HwALLOWED_TCP_IN=22 443

# Especifica si realmente el Honeywall restringirá la red de salida
# Conexiones a puertos de destino específicos.
# [Valid argument: yes | no]
HwRESTRICT=yes

# Especifica los puertos de destino TCP Honeypots puede enviar el tráfico de red.
# [Valid argument: space delimited list of UDP ports]
HwALLOWED_TCP_OUT=22 25 43 80 443

# Especifica los UDP los puertos de destino Honeypots pueden enviar el tráfico de red.
# [Valid argument: space delimited list of UDP ports]
HwALLOWED_UDP_OUT=53 123

# Especifica si realmente comenzar el alertar de correo electrónico y la muestra.
# [Valid argument: yes | no]
HwALERT=yes

# Especifica dirección de correo electrónico para usar para alertar de correo electrónico.
# [Valid argument: any email address]
HwALERT_EMAIL=

# NIC Module List - El juego esto al número y la orden usted desea
# para cargar drivers NIC, tal que usted consigue la orden usted quieren
# para eth0, eth1, eth2, etc.
# [Valid argument: list of strings]
#
# Example: eeepro100 8139too
HwNICMODLIST=

# Lista negra, lista Blanca, y Fencelist (registrar y bloquear).
# [Valid argument: string ]
HwFWBLACK=/etc/blacklist.txt

# [Valid argument: string ]
HwFWWHITE=/etc/whitelist.txt

# [Valid argument: string ]
HwFWFENCE=/etc/fencelist.txt

```

```

# [Valid argument: yes | no]
HwBWLIST_ENABLE=no

# [Valid argument: yes | no]
HwFENCELIST_ENABLE=no

# La siguiente característica permite al roo para permitir a atacantes en el
# Honeypots pero ellos no pueden enviar paquetes...
# [Valid argument: yes | no]
HwROACHMOTEL_ENABLE=no

# Incapacita BPF la filtración de basado en el contenido HwHPOT_PUBLIC_IP
# y la lista blanca y negra contenida dentro HwFWBLACK y HwFWWHITE
# si la HwBWLIST_ENABLE es on.
# [Valid argument: yes | no]
HwBPF_DISABLE=no

# Esta capacidad aún no es puesta en práctica en roo.
# [Valid argument: string ]
# Example: -c 1 -m 16 -d
HwHWPARMOPTS=

# Deberíamos cambiar llaves de control y capslock?
HwSWAP_CAPSLOCK_CONTROL=no

#####
# Snort Rule Update Variables
#####
# Permita o incapacite actualizaciones de regla de resoplido automáticas
# [Valid argument: yes | no]
HwRULE_ENABLE=no

# Automáticamente comience de nuevo el resoplido y snort_inline cuando actualizaciones automáticas son
# aplicado y cuándo llamadas de poner al día IDS o reglas de IPS?
# [Valid argument: yes | no]
HwSNORT_RESTART=no

# Oink Code - Requerido por Oinkmaster para recuperar VRT gobiernan actualizaciones
# See: /hw/docs/README.snortrules or
# http://www.honeynet.org/tools/cdrom/roo/manual/
# para instrucciones sobre cómo obtenerlo (Free registration).
# [Valid argument: ~40 char alphanumeric string]
HwOINKCODE=

# El día actualizaciones de regla de resoplido automáticas debería ser recuperado (for weekly updates)
# Para actualizaciones diarias, ponga esto ""
# [Valid argument: sun | mon | tue | wed | thu | fri | sat]
HwRULE_DAY=sat

# La hora de actualizaciones de reglas de resoplido de día debería ser recuperada
# [Valid argument: 0 | 1 | 2 | ... | 23] (0 is Midnight, 12 is noon, 23 is 11PM)
HwRULE_HOUR=3

#####
# Pcap y ajustes de retención de datos DB
# ONLY usado cuando Pcap/DB purge scripts son llamadas
# Pcap/DB data *is NOT* auto purged
#####
# Días para conservar Pcap datos. Esto será usado *IF* /dlg/config/purgePcap.pl
# llaman o retornan NO argumentos.

```

```

HwPCAPDAYS=45

# Días para conservar Pcap datos. Esto será usado *IF* /dlg/config/purgeDB.pl
# llaman o devuelven NO argumentos.
HwDBDAYS=180

#####
# El modo de NAT más es apoyado.

# Espacio lista delimitada de Honeypot ips
# NOTE: DEBE TENER MISMO NÚMERO DE IPS QUE PUBLIC_IP VARIABLE.
# [Valid argument: IP address]
#HwHPOT_PRIV_IP_FOR_NAT=

# Especifica la dirección IP del honeywall's interno (i.e. gateway
# IP for NAT) IP direcciones. Esto sólo es usado en el modo de NAT.
# [Valid argument: IP address ex: 192.168.10.1]
#HwPRIV_IP_FOR_NAT=

# [Valid argument: IP netmask]
#HwALIAS_MASK_FOR_NAT=255.255.255.0

# End of honeywall.conf parameters

#
# Newly defined variables as of Fri Apr 24 10:47:09 GMT 2015
#
HwHFLOW_DB=3
HwSENSOR_ID=1084569134

#
# Newly defined variables as of Sun Apr 26 16:20:02 GMT 2015
#

```

Las configuraciones establecidas en este archivo, reflejan la administración del Honeypot, cada configuración o modificación del archivo crea un registro copia, para que no se pierda la síntesis de control y mantenimiento.

## Menú de diálogos

Usar menús para la configuración es la más adecuada por que se interactúa directamente con el Sistema Honeywall, donde la administración cuenta con seis tipos de acceso que pueden ser modificados para una mejor gestión:

- **Status.**
- OS Administration.
- **Honeywall Administration.**
- **Honeywall Configuration.**



- Documentation.
- Exit

Para poder acceder al menú, se debe ingresar como “root” y el siguiente comando “/dlg/dialogmenu.sh”

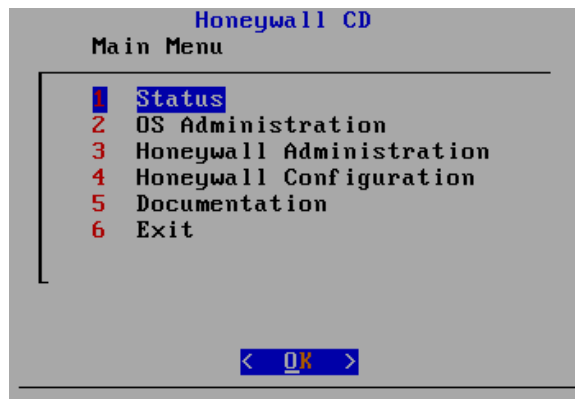


Gráfico 4.3. 6 Menú principal Honeywall

Elaborado por: Javier Vargas

Status: aquí se encuentra el estado actual del Honeywall, las IPs configuradas, alertas, reglas del Firewall, conexiones entrantes y salientes, y la configuración del Honeywall.

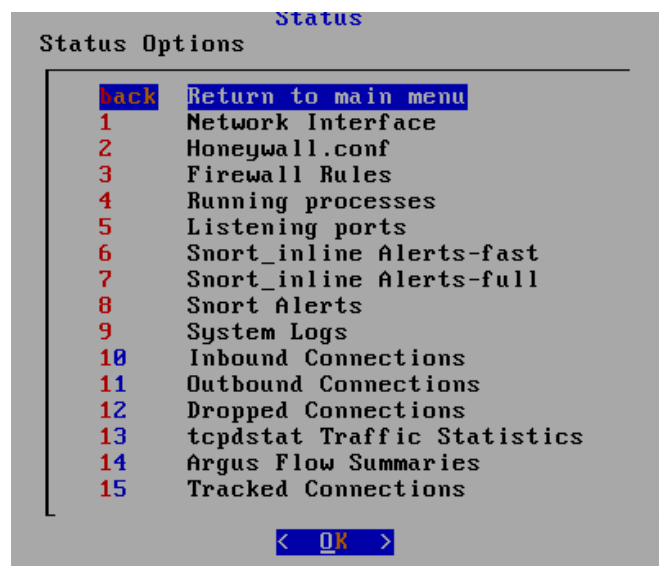


Gráfico 4.3. 7 Menú Informativo del funcionamiento del Honeywall

Elaborado por: Javier Vargas

Honeywall Administration: muy importante las configuración realizadas en los demás menús no se verán reflejadas, debido a la edición de los archivos “.conf”, debido a esto se debe reiniciar el Honeywall en general o se recargan las disposiciones por separado para no detener los servicios prestados o por la actualización de las reglas en las conexiones entrantes y salientes.

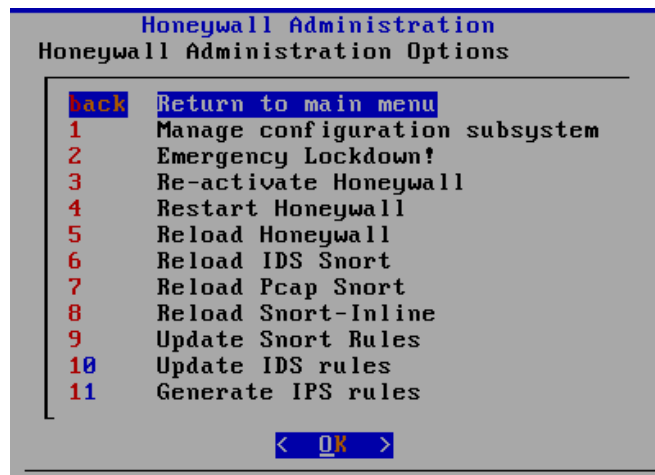


Gráfico 4.3. 8 Menú administrativo del Honeywall.

Elaborado por: Javier Vargas

Honeywall Configuration: contiene la configuración básica del Honeywall, la importancia recae en uso de las reglas y las alertas del Snort\_Inline, además la gestión de las listas negras y blancas (Black list and White list). El tiempo de escaneo se establece en esta sección o menú por medio de “Connection Limiting”, depende funcionalmente de la escala establecida, es horas, TCP/UDP/ICMP determinados por intervalos de tiempo.

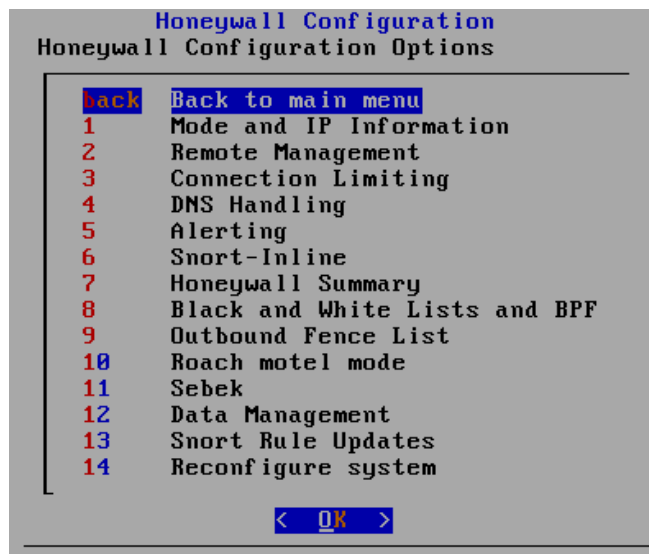


Gráfico 4.3. 9 Menú primordial de configuración Honeywall

Elaborado por: Javier Vargas

## Interfaz del navegador GUI

La administración de los servicios de monitoreo, es accedido por medio del navegador WEB permite un mejor control, ya que se estable una única dirección de acceso, exclusivamente el administrador de red, podrá modificar el Honeywall, consumiendo el Honeypot para poder detectar los tipos de intrusiones existentes en un primer monitoreo, aumentando las reglas del Firewall o bloqueando conexiones malignas hacía la red de datos de la FISEI.

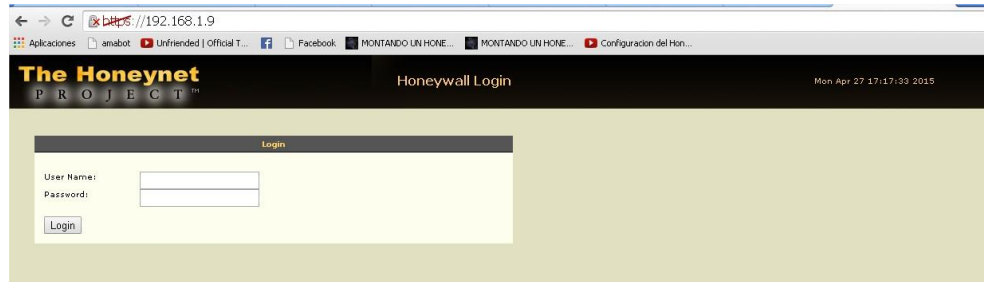
## Walleye

Un Servidor Web accesible por la seguridad que precede por el puerto 443, utilizando listas generadas por el Honeypot, la gestión es controlado por walleye.py archivo de configuración estándar, para el acceso se establece en el archivo “honeywall.conf”, el cual la dirección IP de acceso debe estar restringida por las reglas entrantes y salientes del Honeywall.

Acceso por medio de la URL:

**Https: // dirección-IP-administrador y el Usuario: roo**

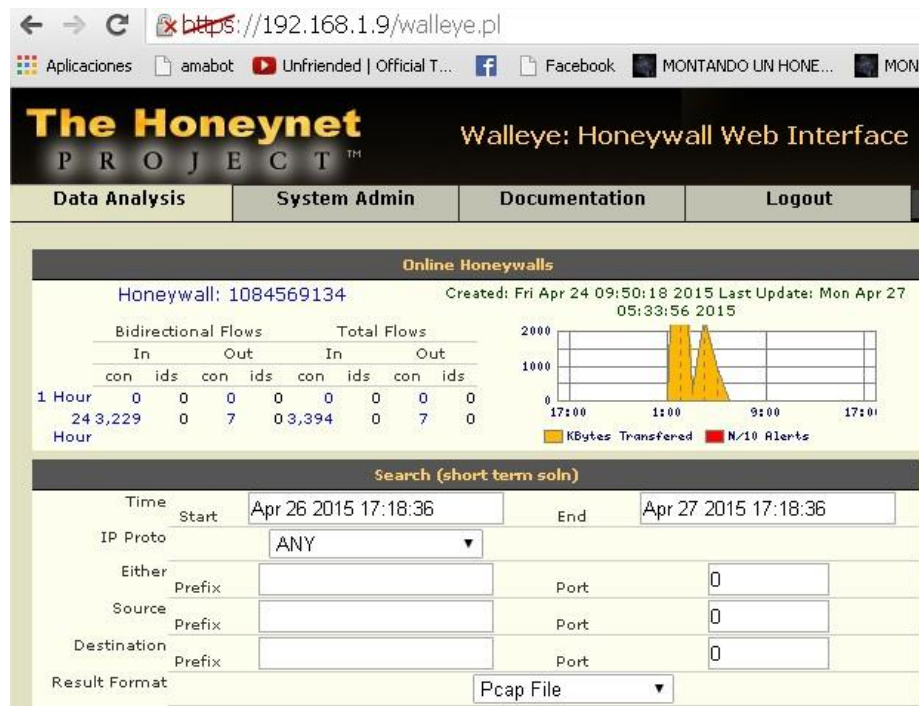
Contraseña: la primera clave de acceso es “honey”, una vez ingresado es necesario cambiar las contraseñas del roo y root.



**Gráfico 4.3. 10 Administrador de interfaz web del Honeywall**

**Elaborado por: Javier Vargas**

Interfaz del administrador Honeywall, se encuentra los módulos de control y análisis de resultados, se establece las fechas almacenando en una base de datos exportable en un archivo “.pcap”.



**Gráfico 4.3. 11 Ventana principal de administración.**

**Elaborado por: Javier Vargas**

#### 4.4 Procesos y Herramientas de la Honeynet

##### Unidades de práctica

EQUIPAMIENTO				
Equipo Físico/Virtual	Dirección IP	Sistema Operativo	Versión	Observaciones
<b>Físico</b>	192.168.1.6	Fedora	21	Utilizado para la virtualización de las maquinas: Honeywall, CentOS, Windows XP, Kali Linux.
<b>Virtual</b>	192.168.1.10	CentOS	6.5	Utilizado para configurarse como Honeypot
<b>Virtual</b>	192.168.1.9	Windows 7	Service Pack 3	El Sistema Operativo varia, solo se utiliza para la administración del Honeywall.
<b>Virtual</b>	192.168.1.20	Windows XP	Service Pack 1	Configurado para dos opciones: Sebek Cliente Ataques en un ambiente controlado.
<b>Virtual</b>	192.168.1.21	Kali Linux	1.1.0a	Sistema Operativo utilizado como medio de análisis del Honeywall, por la gran variedad de herramientas que este posee.

Tabla 4.4. 1 Equipamiento necesario para la red Honeynet

Elaborado por: Javier Vargas

SOFTWARE				
Herramienta	Versión	Descripción	Nivel de Acceso	Usuario y Privilegio
<b>Honeywall</b>	Roo1.4	Utilizado para el proyecto de investigación.	Nivel C2	Honeywall; roo y root: administrador.
<b>Sebek</b>	Win32-3.0.5	La herramienta Sebek es utilizada para configurar el cliente del Honeywall.	Nivel C1	Tester: acceso al SO como administrador.
<b>Wireshark</b>	1.12.4	Se utiliza para tabular y presentar los resultados obtenidos en los primeros análisis del Honeywall.	Nivel C2 y Nivel B1	Tester: acceso por autor del proyecto.
<b>Kali Linux: nmap sqlmap metasploit framework intrace</b>	1.1.0a	Las herramientas se utilizan para acceder al Honeypot por pruebas de “Penetration Testing Training”.	Nivel D y Nivel B2	Tester

**Tabla 4.4. 2 Software utilizado monitoreo y control**

**Elaborado por: Javier Vargas**

Un Honeypot montado en la red de la Honeynet, se instala con las configuraciones básicas, con el objetivo de simular los servicios prestados por el o los Servidores de la red de la FISEI, la distribución implementada para el proyecto de Investigación es CentOS con los siguientes servicios:

- NetworManager (Administración de Red): Servicio primordial en el Servidor, contiene la configuración completa de Red.

- DNS (Sistema de Nombres de Dominio): El servicio dns en CentOS, trae BIND (Berkeley Internet Name Domain), existiendo una ejecución del protocolo y manejando componentes como named (nombres de dominio del sistema), zonas de dominio y herramientas de verificación del correcto funcionamiento del DNS BIND.
- Dovecot: Un Servidor de IMAP y POP3, protocolos para correo y mensajería previamente configurados en el Servidor.
- SSH (Shell Seguro): Protocolo de comunicación segura.
- Http (Protocolo de transferencia de hipertexto): Configurado mediante el uso de nombres de dominio, para la resolución de nombres.
- Base de Datos: Un Servidor se establece por prestar servicios uno de ellos de gran jerarquía es el acceso a una base de datos, la seguridad se presta a la gestión del gestor de base de datos, para el cual se implantó POSTGRESQL, un sistema de gestión de base de datos relacional.

Los servicios comúnmente configurados en los Servidores de la red, el porqué de estos servicios, cada servicio cuentan con su sistema de protección, el atacante pretenderá ingresar al Sistema, la mentalidad de un atacante o intruso informático, “el poder acceder a los sistemas seguros que puedan existir”. Configuración de los servicios del sistema trampa ver **Anexo A2**.

## **Herramientas de análisis e intrusión**

Existen una variedad de ataques citaremos los más conocidos:

### **Ataque de fuerza bruta**

Se explotan una gran cantidad de vulnerabilidades, permitiendo al atacante poder ingresar a un Sistema Operativo, aplicación o servicios, con métodos que pueden ser, el uso de Scripts (archivo de órdenes), enviando una serie de combinaciones que contienen una lista grande de usuarios, contraseñas y variedad de combinaciones para poder acceder.

### **Ataques de denegación de servicios**

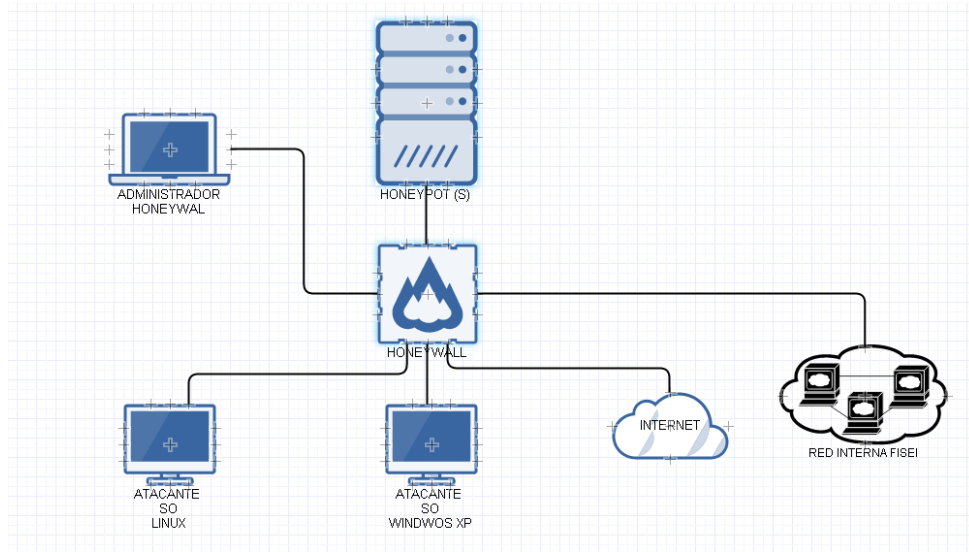
Un ataque de DDoS (Denegación de servicios), se orienta a los Sistemas de computadores o como objetivo secundario poder acceder a una red de datos privada, el método es que un servicio o recurso consumido por el sistema se negado o bloqueado, obligando al administrador del Servidor a reiniciar el servicio, pero cuando el servicio es detenido el atacante detecta un posible acceso al sistema.

### **Ataque Man-in-the-middle**

Es un tipo de ataque más utilizado, su objetivo principal es el escaneo de puertos, permitiendo al atacante conocer los paquetes enviados en la red, con la información que se obtiene de ciertos paquetes, fácilmente se puede acceder a un sistema, en las redes circula una gran variedad de información, al ser capturada puede ser usada para ataques dañinos al sistema.



## Escenarios controlados de ciberataques



**Gráfico 4.4. 1 Honeywall como intermediaron de conexión.**

**Elaborado por: Javier Vargas**

El diagrama simula posibles atacantes a nuestro Honeypot, los atacantes pueden encontrar una gran variedad de medios de acceso a la red de datos, el ciberataque puede ser por medio de la red interna (red FISEI) o externa (Internet), El HoneyWall actuaría como un Firewall, permitiendo o restringiendo las conexiones hacia los Servidores que podemos encontrar en la red de datos, en el caso de estudio del proyecto, se monta un Servidor Honeypot que actúa como Sistema trampa, engañando al atacante como un Sistema vulnerable, inmediatamente el Honeywall envía las alertas al administrador de red, para establecer medidas como:

- Análisis de la IP del atacante.
- Técnicas utilizadas por el atacante.
- Información de los servicios vulnerados.
- Detención y sondeo de la IP del atacante.
- Creación y modificación de las reglas en el Firewall local.
- Aplicación de las políticas de seguridad informática de la FISEI.

**Kali Linux para pruebas de penetración hacia el Honeypot.**

## Nmap

Herramienta utilizada para el mapear redes de datos, pero también es utilizada por los atacantes o administradores de red para explotación de la información de un Sistema, este tipo de mapeo envía una serie de peticiones al Servidor, manipulando puertos y protocolos que pueda encontrar.

Pruebas de conectividad entre el “Atacante” y el Honeypot

```
root@kali:~# ping 192.168.1.10
PING 192.168.1.10 (192.168.1.10) 56(84) bytes of data:
64 bytes from 192.168.1.10: icmp_req=1 ttl=64 time=1.19 ms
64 bytes from 192.168.1.10: icmp_req=2 ttl=64 time=0.515 ms
64 bytes from 192.168.1.10: icmp_req=3 ttl=64 time=0.484 ms
64 bytes from 192.168.1.10: icmp_req=4 ttl=64 time=0.439 ms
64 bytes from 192.168.1.10: icmp_req=5 ttl=64 time=0.564 ms
64 bytes from 192.168.1.10: icmp_req=6 ttl=64 time=0.517 ms
64 bytes from 192.168.1.10: icmp_req=7 ttl=64 time=2.25 ms
```

Gráfico 4.4. 2 Pruebas de conectividad. Kali Linux

Elaborado por: Javier Vargas

Uso de nmap con los siguientes parámetros:

- O: obtener información detalla del SO
- sV: escaneo de puertos.
- sS: para un escaneo sigiloso.

```

root@kali:~# nmap -O 192.168.1.10

Starting Nmap 6.47 ( http://nmap.org ) at 2015-04-29 09:49 CEST
Nmap scan report for 192.168.1.10
Host is up (0.00082s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
111/tcp   open  rpcbind
5432/tcp  open  postgresql
MAC Address: 08:00:27:05:B9:EE (Cadmus Computer Systems)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.01 seconds

```

**Gráfico 4.4. 3 Escaneo mediante nmap -O.**

**Elaborado por: Javier Vargas**

Análisis con la herramienta nmap instalada en Kali Linux, utilizado para pruebas de Testing en un ambiente controlado, información detalla del SO.

```

root@kali:~# nmap -sV 192.168.1.10

Starting Nmap 6.47 ( http://nmap.org ) at 2015-04-29 09:46 CEST
Nmap scan report for 192.168.1.10
Host is up (0.00064s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 5.3 (protocol 2.0)
53/tcp    open  domain
111/tcp   open  rpcbind      2-4 (RPC #100000)
5432/tcp  open  postgresql   PostgreSQL DB
1 service unrecognized despite returning data. If you know the service
/version, please submit the following fingerprint at http://www.insecu
re.org/cgi-bin/servicefp-submit.cgi :
SF-Port5432-TCP:V=6.47%I=7%D=4/29%Time=55408C51%P=x86_64-unknown-linux
-gnu
SF:%r(SMBProgNeg,85,"E\0\0\0\x84SFATAL\0C0A000\0Munsupported\x20fronte
nd\x
SF:20protocol\x2065363\ .19778:\x20server\x20supports\x201\ .0\x20to\x20
3\ .0
SF:\0Fpostmaster\ .c\0L1734\0RProcessStartupPacket\0\0");
MAC Address: 08:00:27:05:B9:EE (Cadmus Computer Systems)

Service detection performed. Please report any incorrect results at ht
tp://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.21 seconds

```

**Gráfico 4.4. 4 Escaneo mediante nmap -sV.**

**Elaborado por: Javier Vargas**

Escaneo de puertos “-sV”, exponiendo puertos disponibles y abiertos a cualquier tipo de conexión dentro del Servidor anfitrión.

```
root@kali:~# nmap -A 192.168.1.10
Starting Nmap 6.47 ( http://nmap.org ) at 2015-04-29 09:51 CEST
Nmap scan report for 192.168.1.10
Host is up (0.00072s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE          VERSION
22/tcp    open  ssh              OpenSSH 5.3 (protocol 2.0)
|_ ssh-hostkey:
|_ 1024 d3:c0:67:5e:4e:0d:bf:7a:73:4e:84:19:bf:0d:e1:cf (DSA)
|_ 2048 1a:8e:9e:e2:55:ab:bc:40:3d:3c:12:cd:08:84:c0:12 (RSA)
53/tcp    open  domain
|_ dns-nsid:
|_ bind.version: 9.8.2rc1-RedHat-9.8.2-0.17.rc1.el6_4.6
111/tcp   open  rpcbind         2-4 (RPC #100000)
|_ rpcinfo:
|_  program version  port/proto  service
|_ 100000  2,3,4      111/tcp    rpcbind
|_ 100000  2,3,4      111/udp    rpcbind
|_ 100024  1          45479/udp  status
|_ 100024  1          50704/tcp  status
5432/tcp  open  postgresql      PostgreSQL DB
|_ service unrecognized despite returning data. If you know the service
|_ /version, please submit the following fingerprint at http://www.insecu
|_ re.org/cgi-bin/servicefp-submit.cgi :
|_ SF-Port5432-TCP:V=0.47%I=7%O=4/29%Time=55408D78%P=x86_64-unknown-linux
|_ .gnu
|_ SF-%r(SMBProgNeg,85,"E\0\0\0\84SFATAL\0C0A000\0Munsupported\x20fronte
|_ nd\x
|_ SF:20protocol\x2065363\,19778:\x20server\x20supports\x201\,0\x20to\x20
|_ 3\,0
|_ SF:\0Postmaster\,c\0L1734\0RProcessStartupPacket\0\0");
|_ MAC Address: 08:00:27:05:B9:EE (Cadmus Computer Systems)
|_ Device type: general purpose
|_ Running: Linux 2.6.X|3.X
|_ OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
|_ OS details: Linux 2.6.32 - 3.10
|_ Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.72 ms 192.168.1.10

OS and Service detection performed. Please report any incorrect result
s at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.65 seconds
```

Gráfico 4.4. 5 Escaneo mediante nmap -sS.

Elaborado por: Javier Vargas

Escaneo más detallado del sistema anfitrión, enfocándose en el descubrimiento del puerto 5432 controlado por un gestor de base de datos POSTGRESQL, además se muestra información de la conexión SSH que permite un acceso de tipo remoto. Como primer test hacia el Honeypot, los resultados configurados en el Honeywall para un escaneo por horas, de la IP de Kali Linux: 192.168.1.45, muestra lo siguiente:

## Administración web del Honeywall resultados

Aggregated Flows: Aggregated by dst_ip Observed from Sensor 1084569134 Between Tue Apr 28 15:45:19 2015 and Tue Apr 28 16:45:19 2015														
(Previous Page)		Start		1		End		(Next Page)		1 / 1				
Filter		Aggregate By	Aggregate Totals								Individual Flow Maximums			
Include	Exclude	Destination IP ▼	Flows	Alerts	SRC Ports	DST Ports	SRC pkts	SRC bytes	DST pkts	DST bytes	SRC pkts	SRC bytes	DST pkts	DST bytes
<input type="checkbox"/>	<input type="checkbox"/>	192.168.1.45	18	0	3	18	63	3,611	58	2,591	5	534	6	344
<input type="checkbox"/>	<input type="checkbox"/>	192.168.1.10	9,490	9	8,582	618	60,583	3,349,601	50,524	2,671,246	22	15,689	16	5,360
<input type="checkbox"/>	<input type="checkbox"/>	192.168.1.8	1	0	1	1	1	32	1	32	1	32	1	32
Apply checkbox filters														

Gráfico 4.4. 6 Valores obtenidos en el análisis nmap.

Elaborado por: Javier Vargas

April 2015						
sun	mon	tue	wed	thu	fri	sat
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		
(Prior Month) (Next Month)						
(Prior Year) (Next Year)						
Hour	Cons		IDS			
0:00	0		0			
1:00	0		0			
2:00	0		0			
3:00	0		0			
4:00	0		0			
5:00	0		0			
6:00	0		0			
7:00	0		0			
8:00	0		0			
9:00	0		0			
10:00	0		0			
11:00	0		0			
12:00	714		2			
13:00	641		0			
14:00	4,552		8			
15:00	10,212		0			
16:00	9,505		9			
17:00	0		0			
18:00	0		0			
19:00	0		0			
20:00	0		0			
21:00	0		0			
22:00	0		0			
23:00	0		0			

Gráfico 4.4. 7 Tabulación de resultados por calendario.

Elaborado por: Javier Vargas

El análisis es periódico se registra por calendario (ver Gráfico 4.3. 27), Honeywall tabula los resultados por el número de Cons (término utilizado para interpretar las peticiones o conexiones) entrantes desde esa IP y los IDS, que son las reglas configuradas en el Snort, patentemente se nota un numero grande peticiones hacia el Honeypot, existen reglas básicas configuradas en IDS, pero a su vez se puede incrementar más tipos de reglas para poder un mayor control del sistema.

## Metasploit

Es un mecanismo de seguridad informática, su principal objetivo es explotar las vulnerabilidades que se puede encontrar en un Sistema Operativo, páginas web, base de datos entre otros.

Uso de metasploit con auxiliares para escaneo de vulnerabilidades en



```
root@kali:~# msfconsole
[*] Starting the Metasploit Framework console...

#####
--..;@; @; --..;
" @@@@'..'@ @@@@'..'@ "
- @@@@@@@@@@@@@ @@@@@@@@@@@@@ @;
 .@@@@@@@@@@@@ @@@@@@@@@@@@@
"-'@ @ -.@ @ '-'
"@' ; @ @
| @ @ @ @
' @ @ @ @
'. @ @ @ @
', @ @ @ @
( 3 C ) <|_ Metasploit!
;@' * /|_
'(. . . .)' \|_

Trouble managing data? List, sort, group, tag and search your pentest data
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

=[ metasploit v4.11.1-201503100P [core:4011716,pre:2015031001,api:1.0.0] o hear"
+ -- ==[ 1412 exploits - 802 auxiliary - 229 post ]
+ -- ==[ 361 payloads - 37 encoders - 8 nops ]
+ -- ==[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

Gráfico 4.4. 8 Metasploit como herramienta de explotación de vulnerabilidades.

Elaborado por: Javier Vargas

Top 10 Source Ports			Top 10 Destination Ports		
Port	Connections	IDS events	Port	Connections	IDS events
54161	928	2	80	100	7
54162	922	2	705	5	5
47178	619	2	161	5	5
51253	619	2	53	11,248	2
33914	3	2	5432	7,929	0
65214	704	1	443	603	0
57211	616	1	56564	39	0
43714	3	1	22	30	0
46833	3	1	0	22	0
35083	2	1	111	17	0

**Gráfico 4.4. 9 Primer resultado obtenido por el Honeywall.**

Elaborado por: Javier Vargas

Los resultados ejecutados en una prueba de tipo explotación de vulnerabilidad, incrementan las alertas desde el Honeywall, advirtiendo al administrador, los paquetes enviados desde el metasploit, son configuraciones de código malicioso que el sistema interpreta con archivos de configuración, inéditamente puede acceder al Servidor.

Las pruebas de penetración hacia nuestro Honeypot, no solo son con Sistema Operativos orientados a la Seguridad Informática, puede ser una aplicación de código maligno en cualquier SO o desde cualquier tipo de dispositivo en la red de datos.

### **Windows XP con aplicaciones de denegación de servicios DDoS.**

Pruebas de conectividad entre el “Atacante” y el Honeypot

```
C:\Documents and Settings>ping 192.168.1.10
Haciendo ping a 192.168.1.10 con 32 bytes de datos:
Respuesta desde 192.168.1.10: bytes=32 tiempo=3ms TTL=64
Respuesta desde 192.168.1.10: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.10: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.10: bytes=32 tiempo<1m TTL=64
Estadísticas de ping para 192.168.1.10:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 3ms, Media = 0ms
```

**Gráfico 4.4. 10 Pruebas de conectividad. WindowsXP.**

Elaborado por: Javier Vargas

Utilizando una aplicación para denegación de servicios, que utiliza el envío masivo de paquetes colapsando al Honeypot presente en la red de datos.

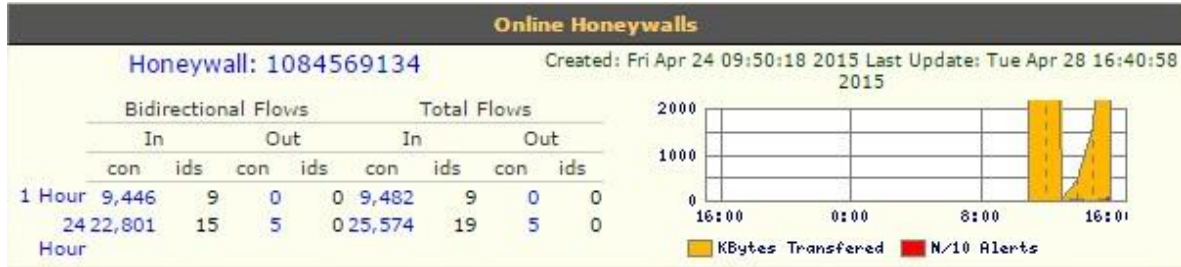


Gráfico 4.4. 11 Resultado diagrama de envío excesivo de paquetes.

Elaborado por: Javier Vargas

Como observamos en el Gráfico 4.4. 11, existe un gran aumento en el tráfico generado por la red de datos, en el envío de paquetes, el administrador de red, inicia el sondeo de la IP entrante causante de este tipo de ataque.

Honeywall en ejecución exploración de las IP que accedieron al Honeypot en la red Honeynet

Activity Report							
Top 10 Honeypots				Top 10 Remote Hosts			
Flags	Host	Connections	IDS events	Host	Connections	IDS events	
	192.168.1.6		4	0	192.168.1.45	18,893	6
	192.168.1.10		1	0	192.168.1.123	3,213	6
					192.168.1.40	725	2
					192.168.1.100	620	2
					192.168.1.8	154	1
					192.168.1.6	1,370	0
					192.168.1.10	65	0
					192.168.1.105	28	0
					192.168.1.200	5	0
					200.210.62.71	1	0

Gráfico 4.4. 12 Honeywall comprometido por varios accesos en la red.

Elaborado por: Javier Vargas

Practica con varios tipos de ataque en un ambiente controlado, se muestra en la tabla “Top 10 Remote Hosts”, donde se visualiza las IPs de los posibles atacantes, los tipos de conexiones entrantes y las reglas accedidas por el IDS, además se observa la tabla “Top 10 Honeypots”, que muestra las IPs de nuestro Honeypot, en toda la red Honeywall.



## Logs del Honeywall

Honeywall cuenta con registro o logs, que permiten al administrador de red, usarlos para poder interpretar más detalladamente el acceso a la red Honeywall, por intermedio del Servidor de protección y control Honeywall, enlistamos los registros de mayor importancia:

### “tcpstat” estadísticas de tráfico generado

DumpFile: /var/log/pcap/1430226061/log

FileSize: 0.20MB

Id: 201504281301

StartTime: Tue Apr 28 13:01:02 2015

EndTime: Tue Apr 28 14:00:58 2015

TotalTime: 3595.40 seconds

TotalCapSize: 0.17MB CapLen: 1315 bytes

# of packets: 2336 (171.94KB)

AvgRate: 1.09Kbps stddev:1.87K PeakRate: 78.26Kbps

### IP flow (unique src/dst pair) Information ###

# of flows: 7 (avg. 333.71 pkts/flow)

Top 10 big flow size (bytes/total in %):

27.9% 7.7% 7.2% 4.4% 4.0% 0.1% 0.1%

### IP address Information ###

# of IPv4 addresses: 5

Top 10 bandwidth usage (bytes/total in %):

100.0% 62.9% 28.9% 7.8% 0.4%

### Packet Size Distribution (including MAC headers) ###

<<<<

[ 32- 63]: 1507

```
[ 64- 127]:    791
[ 128- 255]:   12
[ 256- 511]:   12
[ 512- 1023]:  10
[ 1024- 2047]:  4
```

```
>>>>
```

```
### Protocol Breakdown ###
```

```
<<<<
```

protocol	packets	bytes	bytes/pkt
[0] total	2336 (100.00%)	176064 (100.00%)	75.37
[1] ip	913 ( 39.08%)	90684 ( 51.51%)	99.33
[2] tcp	169 ( 7.23%)	26216 ( 14.89%)	155.12
[3] http(s)	3 ( 0.13%)	192 ( 0.11%)	64.00
[3] http(c)	5 ( 0.21%)	306 ( 0.17%)	61.20
[3] https	161 ( 6.89%)	25718 ( 14.61%)	159.74
[2] udp	639 ( 27.35%)	52850 ( 30.02%)	82.71
[3] dns	639 ( 27.35%)	52850 ( 30.02%)	82.71
[2] icmp	105 ( 4.49%)	11618 ( 6.60%)	110.65

Este registro guarda la información más detallada por cada atacante de red, fichas como dirección MAC, tamaño de los paquetes transmitidos y una lista detallada de los protocolos utilizados.

### Conexiones entre el Honeywall y Honeypot.

“**Inbound Connections**”, registra todas las conexiones entrantes y salientes a /var/log/messages, usando a Snort para la captura de las cargas útiles de actividad de la red y lleno de paquetes en la interfaz de red interna (eth0 defecto), además registra lo que se envía en los paquetes UDP como un proceso del Snort adicional.

Apr 28 15:28:30 localhost kernel: INBOUND UDP: IN=br0 OUT=br0 PHYSIN=eth0 PHYSOUT=eth1 SRC=169.254.103.61 DST=239.255.255.250 LEN=161 TOS=0x00 PREC=0x00 TTL=1 ID=14387 PROTO=UDP SPT=63027 DPT=1900 LEN=141

Apr 28 15:28:33 localhost kernel: INBOUND UDP: IN=br0 OUT=br0 PHYSIN=eth0 PHYSOUT=eth1 SRC=169.254.103.61 DST=239.255.255.250 LEN=161 TOS=0x00 PREC=0x00 TTL=1 ID=14388 PROTO=UDP SPT=63027 DPT=1900 LEN=141

Apr 28 15:29:29 localhost kernel: INBOUND UDP: IN=br0 OUT=br0 PHYSIN=eth0 PHYSOUT=eth1 SRC=169.254.103.61 DST=239.255.255.250 LEN=161 TOS=0x00 PREC=0x00 TTL=1 ID=14393 PROTO=UDP SPT=63027 DPT=1900 LEN=141

Apr 28 15:29:32 localhost kernel: INBOUND UDP: IN=br0 OUT=br0 PHYSIN=eth0 PHYSOUT=eth1 SRC=169.254.103.61 DST=239.255.255.250 LEN=161 TOS=0x00 PREC=0x00 TTL=1 ID=14394 PROTO=UDP SPT=63027 DPT=1900 LEN=141

Apr 28 15:29:33 localhost kernel: INBOUND UDP: IN=br0 OUT=br0 PHYSIN=eth0 PHYSOUT=eth1 SRC=169.254.103.61 DST=169.254.255.255 LEN=240 TOS=0x00 PREC=0x00 TTL=128 ID=14395 PROTO=UDP SPT=138 DPT=138 LEN=220

Apr 28 15:29:35 localhost kernel: INBOUND UDP: IN=br0 OUT=br0 PHYSIN=eth0 PHYSOUT=eth1 SRC=169.254.103.61 DST=239.255.255.250 LEN=161 TOS=0x00 PREC=0x00 TTL=1 ID=14396 PROTO=UDP SPT=63027 DPT=1900 LEN=141

Apr 28 15:29:36 localhost kernel: INBOUND UDP: IN=br0 OUT=br0 PHYSIN=eth0 PHYSOUT=eth1 SRC=169.254.103.61 DST=224.0.0.252 LEN=50 TOS=0x00 PREC=0x00 TTL=1 ID=14397 PROTO=UDP SPT=65508 DPT=5355 LEN=30

Apr 28 15:29:37 localhost kernel: INBOUND UDP: IN=br0 OUT=br0 PHYSIN=eth0 PHYSOUT=eth1 SRC=169.254.103.61 DST=169.254.255.255 LEN=78 TOS=0x00 PREC=0x00 TTL=128 ID=14398 PROTO=UDP SPT=137 DPT=137 LEN=58

Apr 28 15:35:41 localhost kernel: INBOUND UDP: IN=br0 OUT=br0 PHYSIN=eth0 PHYSOUT=eth1 SRC=169.254.103.61 DST=239.255.255.250 LEN=161 TOS=0x00 PREC=0x00 TTL=1 ID=14410 PROTO=UDP SPT=63027 DPT=1900 LEN=141

Apr 28 15:35:44 localhost kernel: INBOUND UDP: IN=br0 OUT=br0 PHYSIN=eth0 PHYSOUT=eth1 SRC=169.254.103.61 DST=239.255.255.250 LEN=161 TOS=0x00 PREC=0x00 TTL=1 ID=14411 PROTO=UDP SPT=63027 DPT=1900 LEN=141

Apr 28 15:35:47 localhost kernel: INBOUND UDP: IN=br0 OUT=br0 PHYSIN=eth0 PHYSOUT=eth1 SRC=169.254.103.61 DST=239.255.255.250 LEN=161 TOS=0x00 PREC=0x00 TTL=1 ID=14412 PROTO=UDP SPT=63027 DPT=1900 LEN=141

.....

## Resultados

Fecha de registro: Apr 28 15:35:47

Host: localhost

Conexiones entrantes (INBOUND UDP): IN=br0 OUT=br0

Tarjetas de red: PHYSIN=eth0 PHYSOUT=eth1

Protocolo de conexión: UDP

Un registro de gran tamaño, ya que almacena información de la fecha de análisis, el protocolo, la conexión entrante y saliente, la dirección física de ingreso, Específica desde donde se envía y hacia dónde se envía.

### Restricciones desde de un previo análisis

Existen dos tipos de restricciones que administrador de red, utiliza para detección y prevención de los ciberataques, las cuales son:

- Listas negras y blancas.
- Reglas del Snort.

Estas dos restricciones, serán modificadas, dependiendo del análisis generado hacia el Honeypot.

### Listas negras y blancas

Son básicamente listas de direcciones IPs, que tendrán acceso hacia la red y por otro lado las direcciones que serán bloqueadas o analizadas con mayor profundidad.

**Black and White List Variables**

In many large or busy networks, there may be alot of production traffic going to the honeypots that you want your honeywall to ignore. Black and white listing allow you to do that. Black listing means *Drop and Ignore*. White listing means *Allow and Ignore* . This effects primarily the firewall.

[Upload Black List file](#) [Upload White List file](#)

Filename containing the IPs or networks to drop and ignore:

Filename containing the ips or networks to ignore:

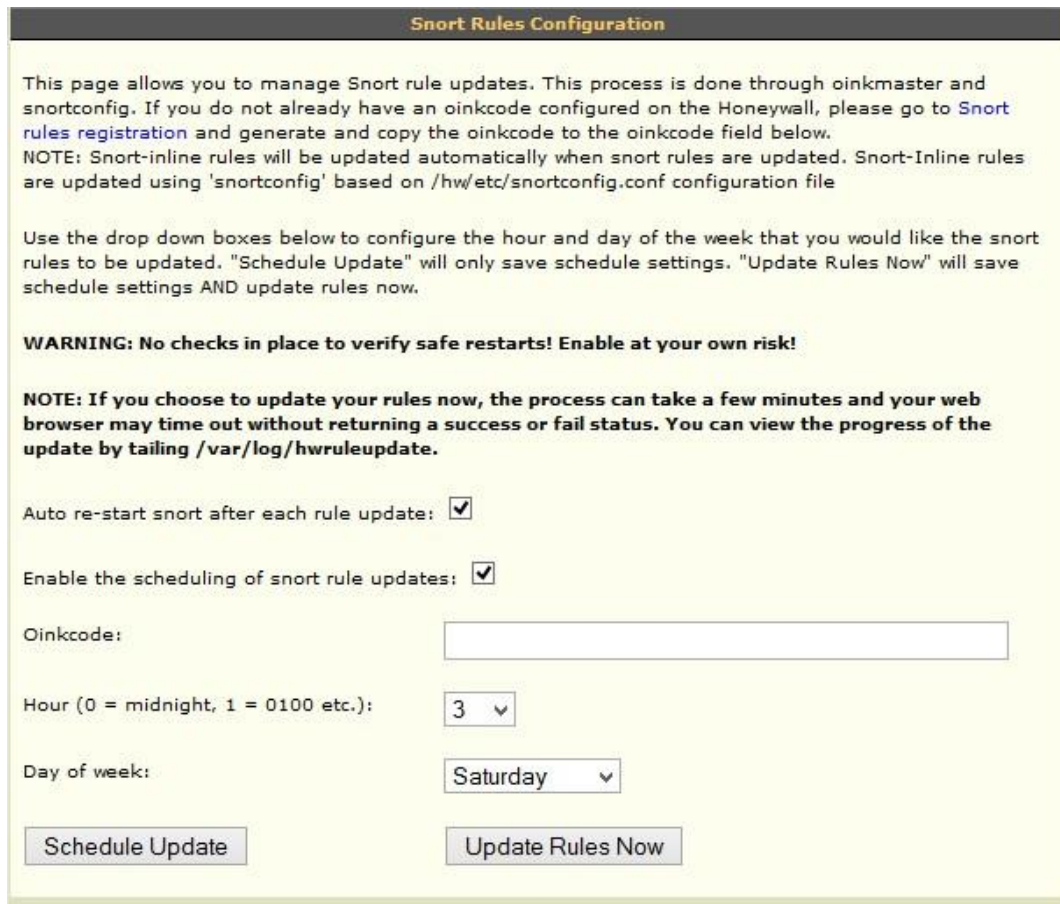
Enable Black and White List.

Gráfico 4.4. 13 Listas de conexiones hacia y desde el Honeywall.

Elaborado por: Javier Vargas

## Reglas del Snort.

Estas reglas son de gran importancia para un sistema seguro contra ataques, las reglas se pueden actualizar periódicamente, en la página oficial de Snort se puede encontrar una gran variedad de reglas permitiendo así al Honeywall incrementar sus seguridades.



The screenshot shows a web interface titled "Snort Rules Configuration". It contains the following elements:

- Header:** "Snort Rules Configuration"
- Text:** "This page allows you to manage Snort rule updates. This process is done through oinkmaster and snortconfig. If you do not already have an oinkcode configured on the Honeywall, please go to [Snort rules registration](#) and generate and copy the oinkcode to the oinkcode field below. NOTE: Snort-inline rules will be updated automatically when snort rules are updated. Snort-Inline rules are updated using 'snortconfig' based on /hw/etc/snortconfig.conf configuration file"
- Text:** "Use the drop down boxes below to configure the hour and day of the week that you would like the snort rules to be updated. 'Schedule Update' will only save schedule settings. 'Update Rules Now' will save schedule settings AND update rules now."
- Warning:** "WARNING: No checks in place to verify safe restarts! Enable at your own risk!"
- Note:** "NOTE: If you choose to update your rules now, the process can take a few minutes and your web browser may time out without returning a success or fail status. You can view the progress of the update by tailing /var/log/hwruleupdate."
- Form Fields:**
  - Auto re-start snort after each rule update:
  - Enable the scheduling of snort rule updates:
  - Oinkcode:
  - Hour (0 = midnight, 1 = 0100 etc.):
  - Day of week:
- Buttons:** "Schedule Update" and "Update Rules Now"

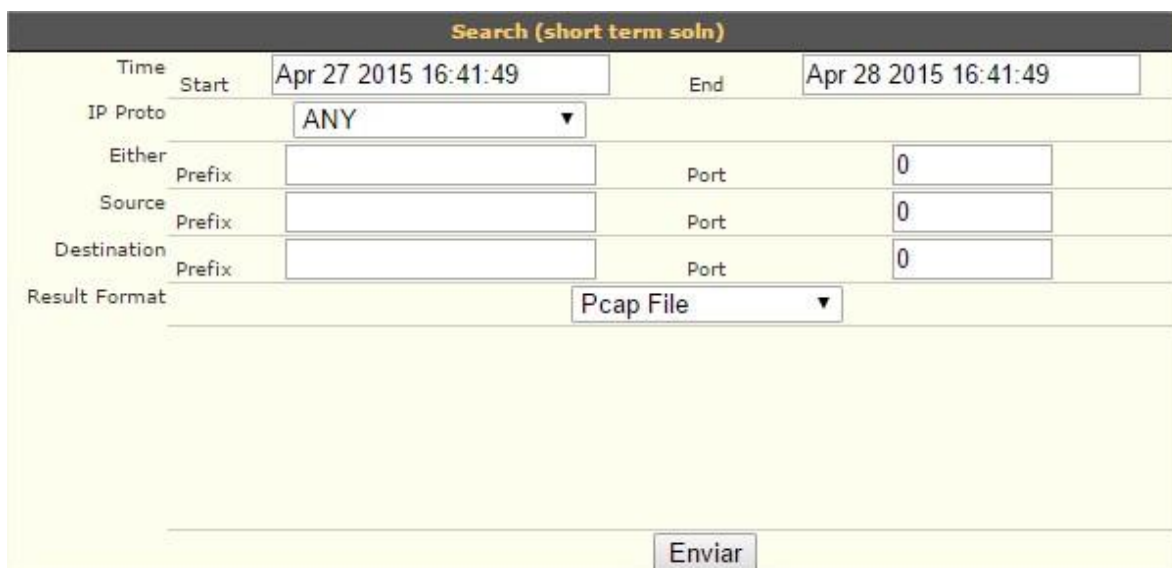
Gráfico 4.4. 14 Administrador de las reglas de Snort.

Elaborado por: Javier Vargas

En el estudio del proyecto se examinó por el uso de reglas de gran complejidad para el control del Honeywall de los IPs entrantes. Paquete analizado en nuestro Honeywall: [snortrules-snapshot-2972.tar.gz](#). La comunidad Snort permite el libre acceso a las reglas, además permitiendo aportar con más reglas o pautas, claramente analizadas por el sistema de protección.

#### 4.5 Resúmenes presentados por el Honeywall (Honeywall)

Para la interpretación de resultados, del administrador HoneyWall, genera un archivo con extensión “.pcap”, que es una aplicación de programación para la captura de paquetes.



The screenshot shows a search interface titled "Search (short term soln)". It includes the following fields:

- Time:** Start: Apr 27 2015 16:41:49, End: Apr 28 2015 16:41:49
- IP Proto:** ANY
- Either:** Prefix: [empty], Port: 0
- Source:** Prefix: [empty], Port: 0
- Destination:** Prefix: [empty], Port: 0
- Result Format:** Pcap File

An "Enviar" button is located at the bottom right of the form.

Gráfico 4.5. 1 Módulo para guardar los análisis presentados en el Honeywall.

Elaborado por: Javier Vargas

Para la tabulación de resultados se utilizó la herramienta Wireshark, analizador de paquetes en las redes de datos. Además Wireshark tiene su propio módulo de escaneo de redes el cual no se utiliza, solamente se manipula un módulo que ayuda a filtrar y crear reglas para tabular los datos obtenidos en el Honeywall y los resultados obtenidos en las pruebas de penetración con el sistema operativo Kali Linux.

#### Resultados derivados por el Honeywall

**Primer análisis Honeywall:** Registro lógico

IP del Servidor: 192.168.1.10

IP del atacante: 192.168.1.6

## Paquetes analizados con destino al Servidor Honeypot:

ARP: Protocolo de resolución de direcciones

Para analizar el protocolo ARP, se escribe en minúsculas arp en el cuadro de filtro y aplicar, entonces solo aparecen paquetes enviados y recibidos de este protocolo.

### Descripción de los parámetros:

- No: se crea un número de identificación por cada entrada a la tabla.
- Time: tiempo máximo de respuesta.
- Source: origen del medio de acceso.
- Destination: destino de consulta.
- Protocol: el protocolo utilizado.
- Length: longitud del paquete.
- Info: información alcanzada.

No.	Time	Source	Destination	Protocol	Length	Info
9	0.901959	CadmusCo_Of:55:3b	HewlettP_88:d1:07	ARP	60	192.168.1.10 is at 08:00:27:0f:55:3b
166	23.391114	HewlettP_88:d1:07	CadmusCo_Of:55:3b	ARP	60	who has 192.168.1.10? Tell 192.168.1.6
167	23.392305	CadmusCo_Of:55:3b	HewlettP_88:d1:07	ARP	60	192.168.1.10 is at 08:00:27:0f:55:3b
177	46.380919	HewlettP_88:d1:07	CadmusCo_Of:55:3b	ARP	60	who has 192.168.1.10? Tell 192.168.1.6
178	46.381228	CadmusCo_Of:55:3b	HewlettP_88:d1:07	ARP	60	192.168.1.10 is at 08:00:27:0f:55:3b
189	73.368319	HewlettP_88:d1:07	CadmusCo_Of:55:3b	ARP	60	who has 192.168.1.10? Tell 192.168.1.6
190	73.368631	CadmusCo_Of:55:3b	HewlettP_88:d1:07	ARP	60	192.168.1.10 is at 08:00:27:0f:55:3b
237	96.360306	HewlettP_88:d1:07	CadmusCo_Of:55:3b	ARP	60	who has 192.168.1.10? Tell 192.168.1.6
238	96.360325	CadmusCo_Of:55:3b	HewlettP_88:d1:07	ARP	60	192.168.1.10 is at 08:00:27:0f:55:3b
469	317.470085	CadmusCo_Of:55:3b	Internet:0f:e7:f0	ARP	60	who has 192.168.1.10? Tell 192.168.1.10 (du...

**Gráfico 4.5. 2 Resultado ARP**

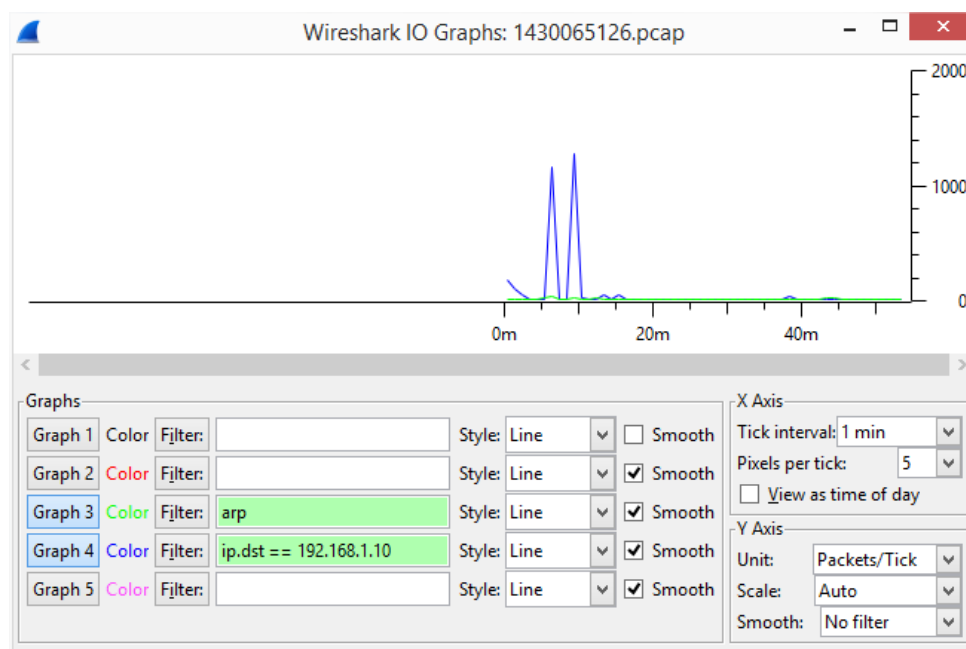
**Elaborado por: Javier Vargas**

En el No 166 se envía desde el Source la MAC (HewlettP\_88:d1:07), pregunta en la red Destination (CadmusCo\_Of:55:3b), con el protocolo ARP, cual es la dirección MAC que se encuentra incorporada a la IP 192.168.1.10, petición enviada desde la IP 192.168.1.6

En el No 167, el Source (CadmusCo\_Of:55:3b), responde a la petición de Destination (HewlettP\_88:d1:07), manifestando que de la dirección IP 192.168.1.10, le corresponde la MAC 08:00:27:0f:55:3b

La información presentada aportaría en la carga de datos, mejorando las consultas los paquetes enviados, pero también se crearían tablas de cache ARP, donde el atacante accedería con facilidad clonando la MAC. Para corregir este depurado de información se limpia las tablas ARP de conexiones temporales.

Grafica detalla del número de petición por el protocolo ARP:



**Gráfico 4.5. 3 Estadísticas ARP.**

**Elaborado por: Javier Vargas**

### **Segundo análisis Honeywall: Registro lógico**

IP del Servidor: 192.168.1.10

IP del atacante: 192.168.1.60

### **Paquetes analizados con destino al Servidor Honeybot:**

ICMP: Protocolo de mensajes de control de Internet

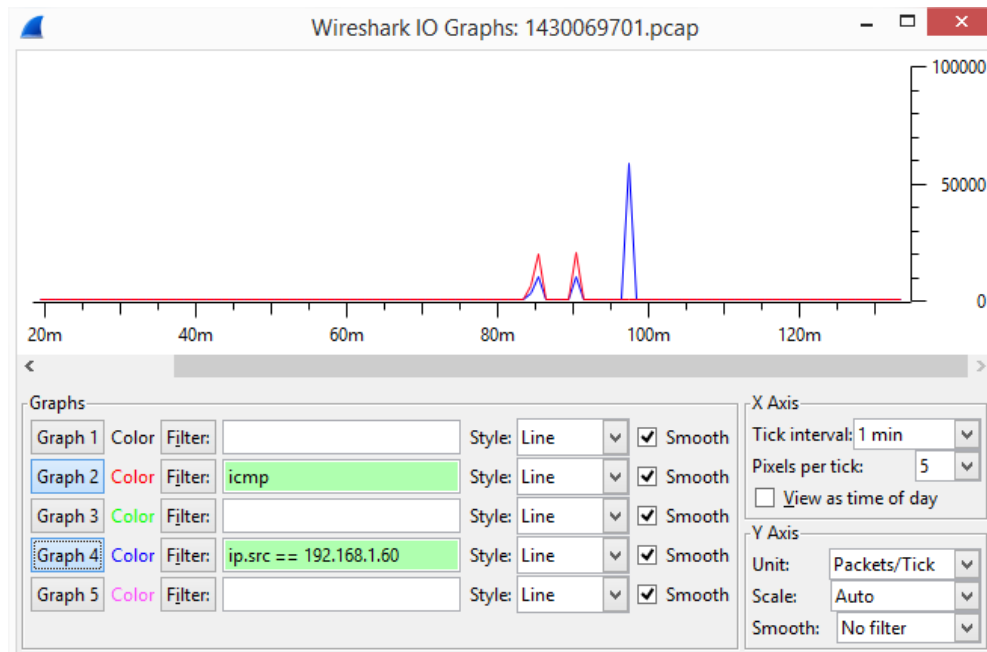
El protocolo ICMP, normalmente es usado en el comando de ejecución ping, donde se envía paquetes comprobando la conectividad de cada uno de ellos, un ataque puede ser la ejecución y envío excesivo de paquetes de gran tamaño, colapsando al Servidor Honeybot.



No.	Time	Source	Destination	Protocol	Length	Info
5962	4678.83371	192.168.1.60	192.168.1.10	ICMP	74	Echo (ping) request id=0x0200, seq=1536/6, ttl=128 (reply in 5963)
5965	4679.82242	192.168.1.60	192.168.1.10	ICMP	74	Echo (ping) request id=0x0200, seq=1792/7, ttl=128 (reply in 5966)
5967	4680.81768	192.168.1.60	192.168.1.10	ICMP	74	Echo (ping) request id=0x0200, seq=2048/8, ttl=128 (reply in 5968)
5969	4681.81752	192.168.1.60	192.168.1.10	ICMP	74	Echo (ping) request id=0x0200, seq=2304/9, ttl=128 (reply in 5970)
6034	5049.30032	192.168.1.60	192.168.1.10	ICMP	74	Echo (ping) request id=0x0200, seq=2560/10, ttl=128 (reply in 6035)
6036	5050.29932	192.168.1.60	192.168.1.10	ICMP	74	Echo (ping) request id=0x0200, seq=2816/11, ttl=128 (reply in 6037)
6038	5051.29455	192.168.1.60	192.168.1.10	ICMP	74	Echo (ping) request id=0x0200, seq=3072/12, ttl=128 (reply in 6039)
6040	5052.29006	192.168.1.60	192.168.1.10	ICMP	74	Echo (ping) request id=0x0200, seq=3328/13, ttl=128 (reply in 6041)
6044	5059.59178	192.168.1.60	192.168.1.10	ICMP	60	Echo (ping) request id=0x0200, seq=3584/14, ttl=254 (reply in 6045)
6046	5059.59554	192.168.1.60	192.168.1.10	ICMP	60	Echo (ping) request id=0x0200, seq=3840/15, ttl=254 (reply in 6047)
6048	5059.59891	192.168.1.60	192.168.1.10	ICMP	60	Echo (ping) request id=0x0200, seq=4096/16, ttl=254 (reply in 6049)
6050	5059.60198	192.168.1.60	192.168.1.10	ICMP	60	Echo (ping) request id=0x0200, seq=4352/17, ttl=254 (reply in 6051)
6052	5059.60489	192.168.1.60	192.168.1.10	ICMP	60	Echo (ping) request id=0x0200, seq=4608/18, ttl=254 (reply in 6053)
6054	5059.60645	192.168.1.60	192.168.1.10	ICMP	60	Echo (ping) request id=0x0200, seq=4864/19, ttl=254 (reply in 6055)
6056	5059.60798	192.168.1.60	192.168.1.10	ICMP	60	Echo (ping) request id=0x0200, seq=5120/20, ttl=254 (reply in 6057)
6058	5059.60977	192.168.1.60	192.168.1.10	ICMP	60	Echo (ping) request id=0x0200, seq=5376/21, ttl=254 (reply in 6059)
6060	5074.51851	192.168.1.60	192.168.1.10	ICMP	60	Echo (ping) request id=0x0200, seq=5632/22, ttl=254 (reply in 6061)
6062	5074.52301	192.168.1.60	192.168.1.10	ICMP	60	Echo (ping) request id=0x0200, seq=5888/23, ttl=254 (reply in 6063)
6064	5074.52752	192.168.1.60	192.168.1.10	ICMP	60	Echo (ping) request id=0x0200, seq=6144/24, ttl=254 (reply in 6065)
6066	5074.52937	192.168.1.60	192.168.1.10	ICMP	60	Echo (ping) request id=0x0200, seq=6400/25, ttl=254 (reply in 6067)
6068	5074.53134	192.168.1.60	192.168.1.10	ICMP	60	Echo (ping) request id=0x0200, seq=6656/26, ttl=254 (reply in 6069)
6070	5074.53347	192.168.1.60	192.168.1.10	ICMP	60	Echo (ping) request id=0x0200, seq=6912/27, ttl=254 (reply in 6071)
6072	5074.53546	192.168.1.60	192.168.1.10	ICMP	60	Echo (ping) request id=0x0200, seq=7168/28, ttl=254 (reply in 6073)
6074	5074.53744	192.168.1.60	192.168.1.10	ICMP	60	Echo (ping) request id=0x0200, seq=7424/29, ttl=254 (reply in 6075)
6076	5074.54002	192.168.1.60	192.168.1.10	ICMP	60	Echo (ping) request id=0x0200, seq=7680/30, ttl=254 (reply in 6077)

**Gráfico 4.5. 4 Resultados ICMP**  
Elaborado por: Javier Vargas

Para solucionar un ataque de tipo básico conocido como “ping de la muerte”, es necesario el bloque o restricción de esta dirección IP, previo a su análisis.  
Grafica detalla del número de petición por el protocolo ICMP:



**Gráfico 4.5. 5 Estadísticas ICMP**  
Elaborado por: Javier Vargas

## Tercer análisis Honeywall: Registro lógico

IP del Servidor: 192.168.1.10

IP del atacante: Variadas IPs

### Paquetes analizados con destino al Servidor HoneyPot:

DNS: Sistema de Nombres de Dominio

El principal servicio configurado en el Servidor es el o los nombres de dominio, las seguridades que conlleva son gestionadas por el administrador del Servidor y las reglas de acceso por el Firewall. Los principales ataques informáticos son dirigidos al DNS del sistema, explotando la información que contiene en su estructura.

No.	Time	Source	Destination	Protocol	Length	Info
767	351.446738	216.218.132.2	192.168.1.10	DNS	119	Standard query response Ox6c44 AAAA 2800:68:a::2
769	351.469140	216.218.132.2	192.168.1.10	DNS	107	Standard query response Ox50b A 201.218.5.10
770	351.685572	199.254.63.254	192.168.1.10	DNS	773	Standard query response Ox324 No such name
772	351.860998	156.154.101.23	192.168.1.10	DNS	531	Standard query response Ox44c
786	353.291677	200.93.227.4	192.168.1.10	DNS	139	Standard query response Ox7e26 A 200.93.227.165
787	353.296690	200.93.227.4	192.168.1.10	DNS	138	Standard query response Ox9e00
802	353.554572	204.145.124.245	192.168.1.10	DNS	606	Standard query response Ox9420 CNAME yonada.postgresql.org RRSIG A 174.143.35.196 RRSIG
805	353.570789	204.145.124.245	192.168.1.10	DNS	518	Standard query response Ox7f06 CNAME yonada.postgresql.org RRSIG AAAA 2001:4800:1501:1::196 RRSIG
806	353.757732	217.196.149.51	192.168.1.10	DNS	811	Standard query response Ox6679 DNSKEY DNSKEY RRSIG
808	353.909529	199.249.112.1	192.168.1.10	DNS	296	Standard query response Oxde10 DS RRSIG
811	354.060550	199.249.112.1	192.168.1.10	DNS	187	Standard query response Ox9e54 DNSKEY DNSKEY DNSKEY DNSKEY RRSIG RRSIG RRSIG
814	354.175689	192.33.4.12	192.168.1.10	DNS	317	Standard query response Ox9e22 DS DS RRSIG
817	354.196656	192.33.4.12	192.168.1.10	DNS	955	Standard query response Ox5975 NS l.root-servers.net NS m.root-servers.net NS f.root-servers.net NS a
819	354.275102	174.143.35.199	192.168.1.10	DNS	426	Standard query response Ox20c5 AAAA 2001:4800:1501:1::196 RRSIG
821	354.281065	174.143.35.199	192.168.1.10	DNS	414	Standard query response Ox0ed9 A 174.143.35.196 RRSIG
999	356.407715	148.251.123.139	192.168.1.10	DNS	142	Standard query response Ox0444
1002	356.407734	148.251.123.139	192.168.1.10	DNS	179	Standard query response Ox3269 A 193.1.193.67
1004	356.515523	192.33.4.12	192.168.1.10	DNS	400	Standard query response Ox2fe4 DS DS DS DS RRSIG
1006	356.518589	192.33.4.12	192.168.1.10	DNS	955	Standard query response Ox72d NS b.root-servers.net NS i.root-servers.net NS a.root-servers.net NS f
1008	356.738358	194.0.37.1	192.168.1.10	DNS	813	Standard query response Ox7913
1010	357.019614	194.0.44.1	192.168.1.10	DNS	1359	Standard query response Ox5c45 DNSKEY DNSKEY DNSKEY DNSKEY DNSKEY RRSIG
1013	357.169093	156.154.100.23	192.168.1.10	DNS	790	Standard query response Ox8987 No such name
1014	357.169099	156.154.100.23	192.168.1.10	DNS	794	Standard query response Ox2e1f No such name

Gráfico 4.5. 6 DNS acceso

Elaborado por: Javier Vargas

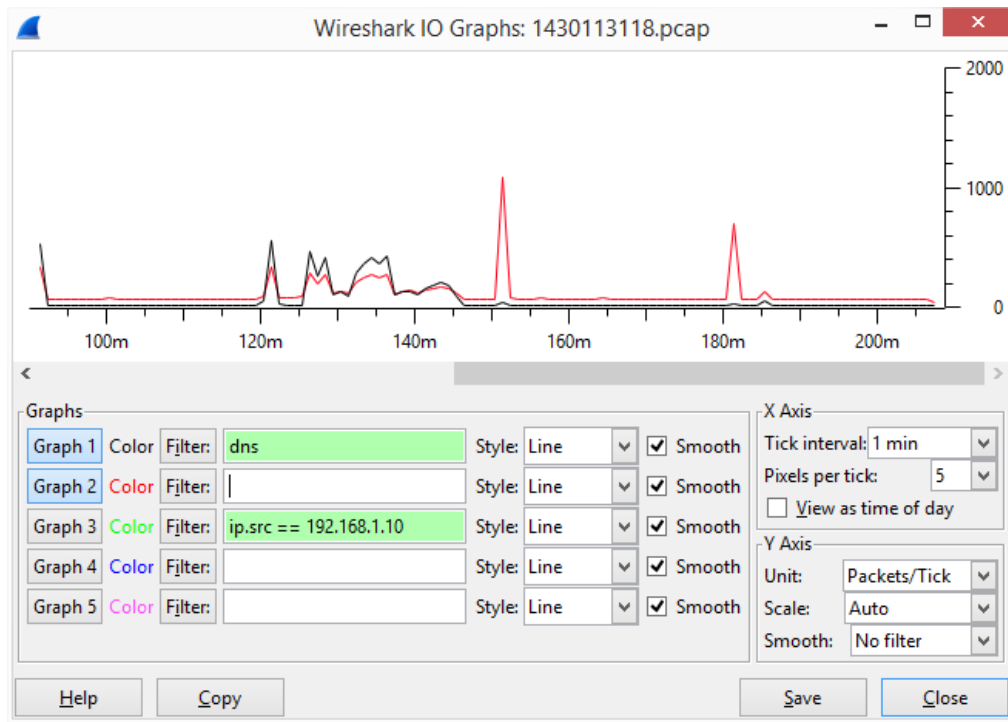
No.	Time	Source	Destination	Protocol	Length	Info
31812	9085.237526	156.154.64.196	192.168.1.10	DNS	294	Standard query response Ox0ca4 A 156.154.66.196
31813	9085.246145	199.6.1.29	192.168.1.10	DNS	978	Standard query response Ox21ef DNSKEY DNSKEY RRSIG RRSIG
31815	9085.273989	156.154.66.196	192.168.1.10	DNS	306	Standard query response Ox7f53 AAAA 2610:a1:1015::e8
31816	9085.547667	199.6.0.29	192.168.1.10	DNS	786	Standard query response Ox710c No such name
31819	9085.701370	216.239.32.10	192.168.1.10	DNS	108	Standard query response Ox0990 AAAA 2607:f8b0:4008:809::200e
31820	9085.728721	216.239.32.10	192.168.1.10	DNS	336	Standard query response Ox7d6e A 186.46.140.108 A 186.46.140.118 A 186.46.140.84 A 186.46.140.103 A 1
31860	9086.509531	216.239.32.10	192.168.1.10	DNS	347	Standard query response Ox748a A 186.46.140.89 A 186.46.140.104 A 186.46.140.118 A 186.46.140.84 A 18
31861	9086.514625	216.239.32.10	192.168.1.10	DNS	113	Standard query response Ox68bb AAAA 2607:f8b0:4008:809::200e
37151	10875.147533	216.239.32.10	192.168.1.10	DNS	143	Standard query response Ox9d6e CNAME clients.l.google.com AAAA 2607:f8b0:4008:807::200e
37153	10875.160454	216.239.32.10	192.168.1.10	DNS	371	Standard query response Ox136e CNAME clients.l.google.com A 186.46.140.103 A 186.46.140.89 A 186.46.1
37154	10875.40954	192.33.14.30	192.168.1.10	DNS	805	Standard query response Ox2391
37157	10875.547641	216.239.32.10	192.168.1.10	DNS	336	Standard query response Oxcd8b A 186.46.140.89 A 186.46.140.119 A 186.46.140.109 A 186.46.140.88 A 18
37158	10875.55605	216.239.32.10	192.168.1.10	DNS	108	Standard query response Ox4f8a AAAA 2607:f8b0:4008:807::200e
37182	10875.961871	216.239.32.10	192.168.1.10	DNS	119	Standard query response Ox5e3c AAAA 2607:f8b0:4008:807::200e
37183	10875.980961	216.239.32.10	192.168.1.10	DNS	347	Standard query response Ox25f A 186.42.100.217 A 186.42.100.221 A 186.42.100.247 A 186.42.100.216 A
38732	11132.93810	201.218.5.3	192.168.1.10	DNS	214	Standard query response Ox2b89 A 201.218.5.10
38733	11132.94071	201.218.5.3	192.168.1.10	DNS	226	Standard query response Oxeba2 AAAA 2800:68:a::2
38736	11133.04916	192.33.4.12	192.168.1.10	DNS	490	Standard query response Ox450a
38738	11133.07243	192.33.4.12	192.168.1.10	DNS	955	Standard query response Oxdcf1 NS e.root-servers.net NS c.root-servers.net NS f.root-servers.net NS k
38739	11133.24639	149.20.64.4	192.168.1.10	DNS	773	Standard query response Ox907c No such name
38741	11133.44659	199.6.1.29	192.168.1.10	DNS	531	Standard query response Ox9316
38757	11134.14856	200.93.227.4	192.168.1.10	DNS	139	Standard query response Ox92b A 200.93.227.165
38758	11134.15005	200.93.227.4	192.168.1.10	DNS	138	Standard query response Ox208
38772	11134.34138	199.249.120.1	192.168.1.10	DNS	520	Standard query response Ox6330
38774	11134.34612	199.249.120.1	192.168.1.10	DNS	520	Standard query response Oxce8f
38777	11134.47141	204.145.124.245	192.168.1.10	DNS	606	Standard query response Ox869d CNAME yonada.postgresql.org RRSIG A 174.143.35.196 RRSIG
38780	11134.49582	204.145.124.245	192.168.1.10	DNS	618	Standard query response Ox5c41 CNAME yonada.postgresql.org RRSIG AAAA 2001:4800:1501:1::196 RRSIG
38783	11134.66504	217.196.149.51	192.168.1.10	DNS	811	Standard query response Ox9b9c DNSKEY DNSKEY RRSIG
38786	11134.89595	213.189.17.231	192.168.1.10	DNS	1502	Standard query response Ox3f30 AAAA 2001:4800:1501:1::196 RRSIG
38787	11134.89721	213.189.17.231	192.168.1.10	DNS	1490	Standard query response Ox4cc A 174.143.35.196 RRSIG
38801	11135.52292	148.251.123.139	192.168.1.10	DNS	179	Standard query response Ox9d24 A 193.1.193.67
38803	11135.52889	148.251.123.139	192.168.1.10	DNS	142	Standard query response Ox417
38806	11135.71084	194.0.6.1	192.168.1.10	DNS	813	Standard query response Ox3d6f
38809	11135.87438	156.154.100.23	192.168.1.10	DNS	790	Standard query response Ox40e1 No such name
38810	11135.88204	156.154.100.23	192.168.1.10	DNS	794	Standard query response Oxcca8 No such name

Gráfico 4.5. 7 DNS acceso 2

Elaborado por: Javier Vargas

Honeywall detecta este tipo de conexiones al Sistema, pero con baja prioridad, el administrador deberá entender los niveles de acceso a la información del DNS.

Grafica detalla del acceso al servicio DNS:



**Gráfico 4.5. 8 Estadística DNS**

**Elaborado por: Javier Vargas**

La tabulación de resultados, permite al administrador de red intuir un poco más de las vulnerabilidades encontradas por los atacantes y los métodos utilizados por los mismo.

Toda la información que obtenemos arrojada en el estudio de investigación del Honeybot en un ambiente controlado, permite claramente tener una visión de los ataques que pueden existir o de los recursos y servicios que pueden ser vulnerados, los resultados deberán ser tratados cuidadosamente ya que se presentan los siguientes factores:

### **Información para el administrador de red.**

Este tipo de información facilita que el administrador de red, aplicar más reglas de protección en su red y saber si un sistemas informático fue accedido deliberadamente por

un atacante, en la investigación se encontró, accesos por puertos y servicios que en el Servidor no se encuentran configurados correctamente, por ejemplo el protocolo SSH, está abierto a cualquier tipo de conexión desde afuera, la pauta de seguridad menciona que las conexiones máximas permitidas deben ser en la red interna del Servidor.

### **Información para el atacante.**

La información que se obtiene del atacante y la información para el atacante es de mayor prioridad, ya que un atacante que tenga acceso a un Honeypot como sistema trampa puede usar la información en contra de la red anfitriona, como se controla este tipo de intrusiones la virtualización de este tipo de Honeypots no solo es uso del Honeypot como herramienta, también interviene el software de virtualización que para el estudio del caso e utiliza VirtualBox.

### **Información de los tipos de ataques.**

Un ataque se presenta en un sistema si el sistema no tiene las debidas protecciones y configuraciones necesarias, para la investigación se utiliza un sistema trampa (Honeypot), permitiendo así estudiar los ataques y herramientas utilizadas por los atacantes, por ejemplo una herramienta de análisis llamada Nmap, permitió el escaneo de puertos abiertos, que a su vez usando otra herramienta, pero usada para hacer ataques como lo es Metasploit.

### **Información de los recursos y servicios**

La información de los recursos accedidos por el atacante, y servicios que este pudo haber vulnerado, permiten determinar si este recurso de red, debe ser mejorado en reglas de seguridad o puede ser detenido o cancelado, por ser una medio peligroso para acceso no autorizado.

### **Información de los Servidores**

La información que un Servidor es de gran importancia, por ejemplo si un servidor es accedido deliberadamente, accede a las bases de datos establecidas en el, para controlar este tipo de intrusiones se reglas o estándares de conexión, permitiendo solo acceder al servido mencionado las IPs o grupos de usuarios permitidos.

## CAPÍTULO 5

### CONCLUSIONES Y RECOMENDACIONES

#### 5.1 Conclusiones

Poseer conocimientos acerca de metodologías y dispositivos de seguridad informática es necesario ya que las TIC'S (Tecnologías de la Información y la Comunicación) avanza y la información que se transmite por los diferentes medios de comunicación son de gran importancia para sus propietarios, por lo que es necesario proteger debidamente.

El manejo de la seguridad informática en los sistemas informáticos de la facultad revela que los componentes no están acordes con las necesidades y requerimientos que ellos tienen para el desarrollo apropiado de su funcionamiento.

Existen varias herramientas que nos permiten monitorear los eventos como lo son mecanismos IDS que es fundamental para monitorear los eventos que se producen dentro de una red revelando información importante de los ataques y atacantes.

Una correcta configuración de la Honeynet red virtual que simula un sistema Firewall o Honeywall, para analiza e interpreta el comportamiento del tráfico en la red de datos, ya que estos brindan control de contenido, denegación de puertos innecesarios y además nos permiten el monitoreo de paquetes dentro de los sistemas informáticos y las red de datos.

## 5.2 Recomendaciones

Realizar análisis habituales de las vulnerabilidades y monitorear continuamente las redes de datos dentro de la facultad, además es necesario establecer protocolos de seguridad para disponer de un mayor control de la seguridad informática en los Servidores y sistemas informáticos.

En la red Honeynet se recomienda implementar más Honeypots, para obtener un análisis más detallado de las vulnerabilidades existentes, los registros deben ser almacenados adecuadamente por la importancia de la información que se obtiene.

Es aconsejable que dentro de la facultad se invierta más proyectos de seguridad informática, por la inseguridad que poseen los sistemas informáticos, ya que la seguridad de la información debe ser considerada como un proceso de mejoramiento continuo, en donde los nuevos requerimientos de seguridad informática se ajusten a los cambios de la facultad.

Se recomienda prácticas de Hacking Ético, denominadas aprender hackeando y no a aprender a hackear, con lo cual se conoce más sobre ataques o atacantes, para poder emitir una respuesta ante posibles ciberataques.

## Bibliografía

- [1] RaulSiles, “Honeynets, conoce a tu enemigo,” Ed. Madrid, Spain, pp 1, 2007.
- [2] L. E. P. D. INGENIERIA SOCIAL: Un ataque a la confianza y al servicio en el sector financiero, “Apuntes de Investigación,” INGENIERIA SOCIAL, Sep 2012.
- [3] O. Bylaws, “The Honeynet Projec,” 01 enero 1999. Disponible en:  
<https://www.honeynet.org/project>.
- [4] P. A. W. Leonardo, “<http://repo.uta.edu.ec/>,” Noviembre 2012. Disponible en:  
<http://repositorio.uta.edu.ec/handle/123456789/2894>.
- [5] S. L. a. M. L. Collin Mulliner, “Poster: HoneyDroid - Creating a Smartphone,” Technische Universit“at Berlin, 2011.
- [6] M. D. Katz, Redes y seguridad, Alfaomega Grupo Editor, pp. pp 1-100 2013.
- [7] X. L. Zongjian Wang, “Intrusion Prevention System Design,” de *Intrusion Prevention System Design*, Springer London, Springer-Verlag London, 2013, pp. pp 375-382.
- [8] Charles Costarella, Sam Chung, Barbara Endicott-Popovsky, David Dittrich, “Hardening Honeynets against Honeypot-Aware Botnet Attacks,” 2013. Disponible en:  
[https://www.tacoma.uw.edu/sites/default/files/sections/InstituteTechnology/C\\_Costarella.pdf](https://www.tacoma.uw.edu/sites/default/files/sections/InstituteTechnology/C_Costarella.pdf).
- [9] Olivier Thonnard, Jouni Viinikka, Corrado Leita, Marc Dacier, “Automating the Analysis of Honeypot Data,” de *Automating the Analysis of Honeypot Data* , Cambridge, MA, USA, Springer Berlin Heidelberg, 2008, pp. pp 406-407.
- [10] K. Graves, CEH : Certified Ethical Hacker Study Guide, USA: Sybex, April 2010.
- [11] L. Spitzner, Honeypots: Tracking Hackers, Universidad de Michigan: Addison-Wesley, 2003 .
- [12] H. C. t. I. Threat, “Lance Spitzner,” *Spitzner*, pp. 2-3, 2008.
- [13] E. CIPHER, “Newsletter of the IEEE Computer Society's TC on Security and Privacy,” Electronic Issue 51, Pacific Grove, CA, USA, pp. 12, 2002.
- [14] K. Sumner, “Honeypots,” Security Architecture, pp. pp 15-20 July 10, 2002 .
- [15] R. M. Magalhaes, Understanding Virtual Honeynets, Ed12, pp 1.. 2003.
- [16] D. O. D. STANDARD, <http://csrc.nist.gov>, Aug 2013.

## Anexos

### ANEXO A1

#### Instalación y Configuración de un Honeywall

Primero en VirtualBox (Crear máquina virtual):

- Nombre Máquina y SO soportado
- Memoria RAM
- Espacio en disco virtual

Tipo de sistema operativo es independiente por que Honeywall, se basa en distribuciones conocidas como son CentOS Y Fedora. La memoria RAM, que se utiliza depende de la capacidad de SO anfitrión, pero como requerimiento mínimo de Honeywall es de 512MB. El tamaño en disco es de gran prioridad, debido a que alojara una gran cantidad de información, lo recomendable es 10GB en disco, para este caso usaremos 20GB.

Antes de iniciar la máquina virtual, se debe crear las tres interfaces de red, debido a que el arranque de Honeywall exige un mínimo de dos tarjetas de red, las tarjetas de red creadas deben ser con distintas MAC y con las configuraciones adecuadas para nuestra red Honeynet.

- Adaptador uno: Host Only
- Adaptador dos: Modo Bridge
- Adaptador tres: Modo Bridge

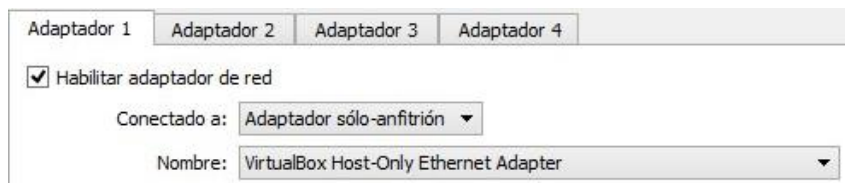


Gráfico A1 1 Adaptador uno



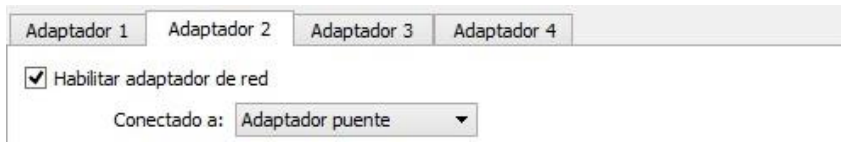


Gráfico A1 2 Adaptador dos

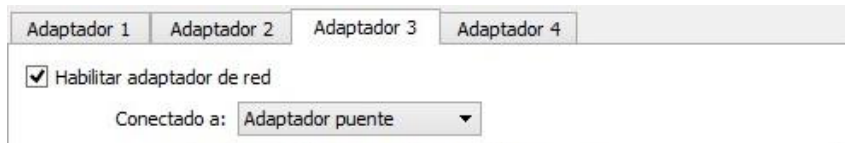


Gráfico A1 3 Adaptador tres.

Una vez concluido la creación de la máquina virtual, podemos iniciar el CD-ROM Honeywall, se lo escoge como medio de arranque CD/DVD.

Ahora se iniciara la ventada principal de “The Honeynet PROJECT”, para poder continuar e iniciar con la instalación presionamos la tecla (Enter).



Gráfico A1 4 HoneyWall

Continuado la instalación, un proceso de instalación empezara a ejecutarse, creando las variables propias de un Linux.

Como es la primera vez que vamos a configurar nuestro Honeywall, se la configuración inicial “/dlg/dialogmenu.sh”

Como primera configuración, debemos leer detenidamente el contrato o licencia, los riesgos que se presentan al instalar este tipo de herramientas son grandes, si no son debidamente controlados por el administrador.

Existen tres métodos de instalación, no está por demás saber el tipo de configuración de cada uno de ellos.

- 1 Floppy: como su nombre dice utiliza un Disquete, como medio de configuración, es útil para configurar rápidamente, pero no se lo utiliza mucho por su antigüedad.
- 2 Defaults: para este tipo de configuración utiliza el valor por defecto de un Honeywall.
- 3 Interview: método que se utilizara para configurar nuestro primer Honeywall, aquí se utiliza el paso a paso.

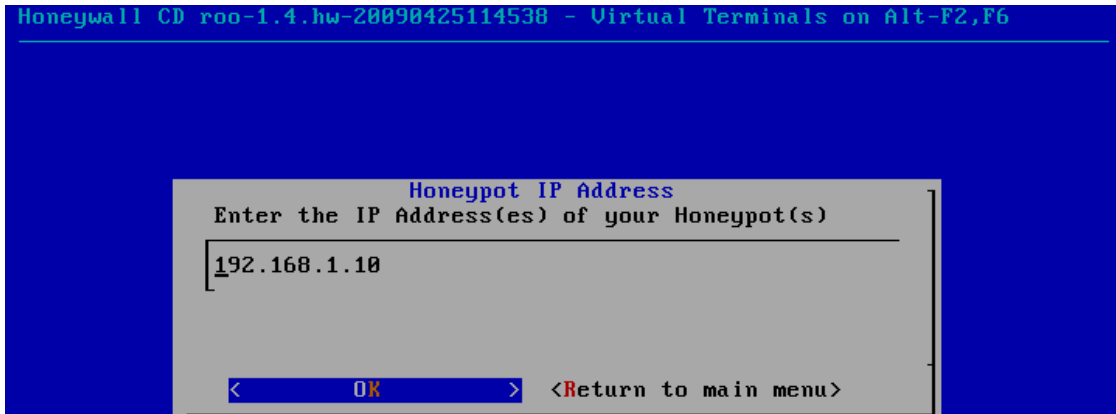


Gráfico A1 5 IP del Servidor Honeywall

Configuración secundaria termina cuando, se inicia la disposición de servicios y puertos accesibles a nuestro Honeywall.

Configuración SSH

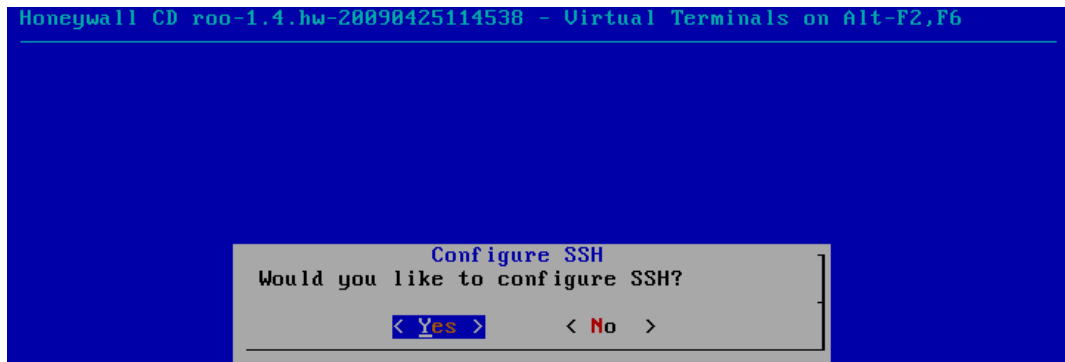


Gráfico A1 6 Configuración del puerto SSH.

SSHD configuración para acceso remoto como root

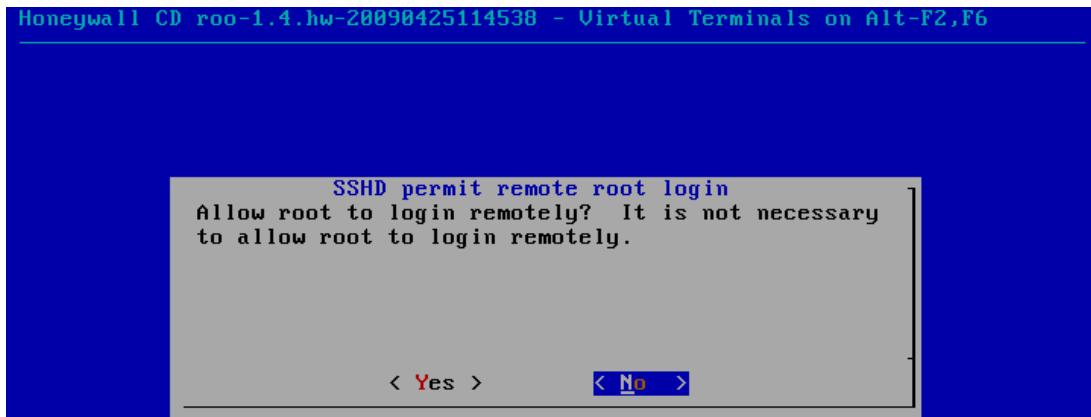


Gráfico A1 7 Acceso al root.

Como paso adicional se configura las contraseñas para acceder solo a la administración por línea de comandos, para poder acceder desde el usuario roo y root, revisar el nivel de seguridad establecidos.

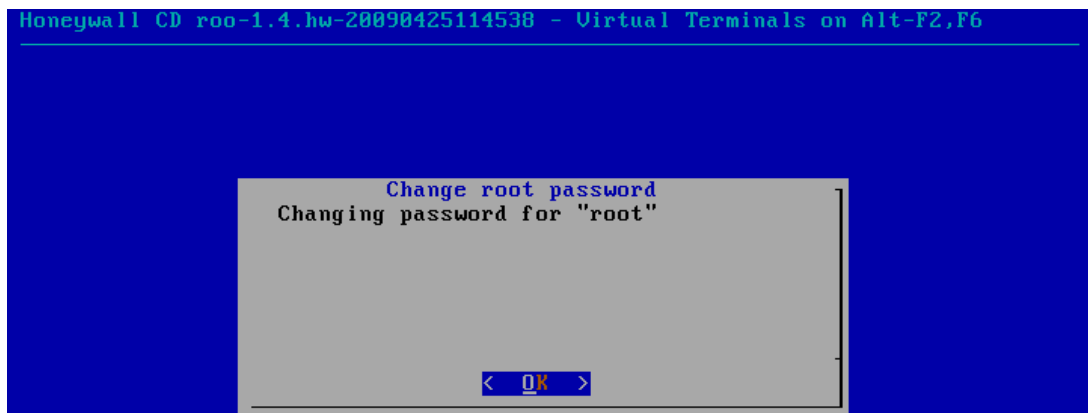


Gráfico A1 8 Modificación de contraseñas.

Administrador del Honeywall debe incluir los puertos 22 y 443 que permiten el acceso remoto y conexión segura para https.

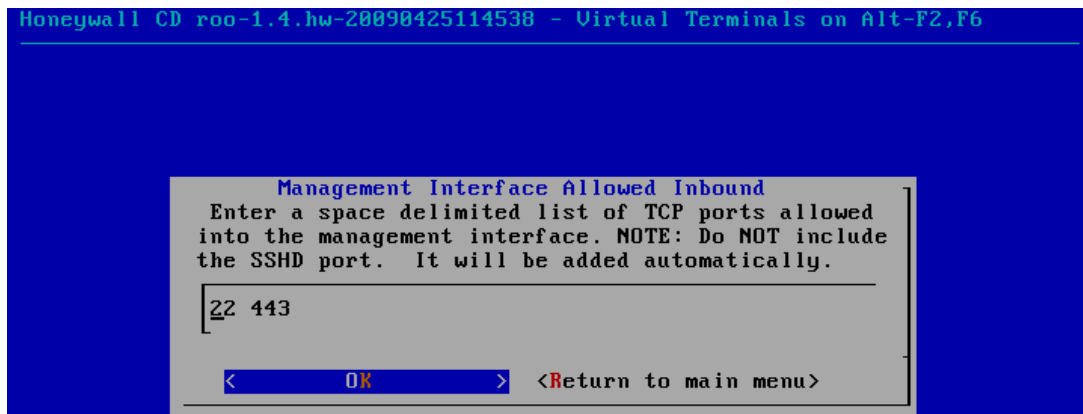


Gráfico A1 9 Puertos de conexión del Honeywall.

Puertos permitidos para salir por el Honeywall para TCP y UDP

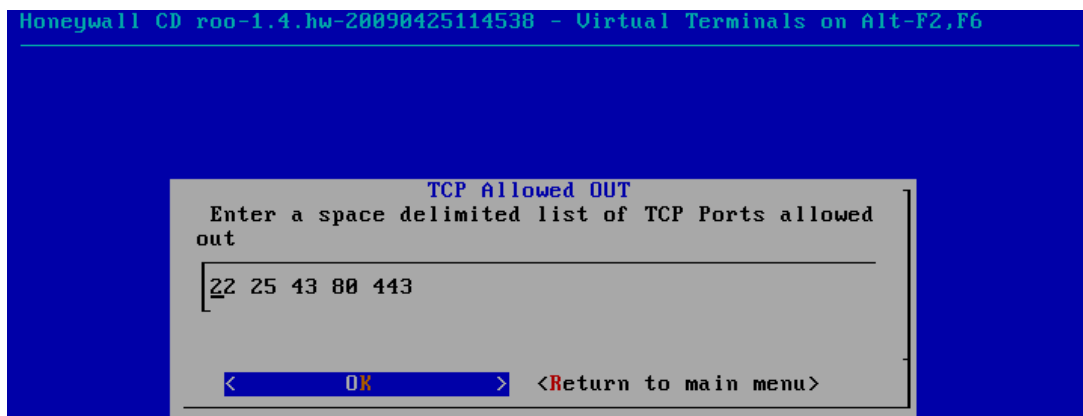


Gráfico A1 10 Puertos escucha.

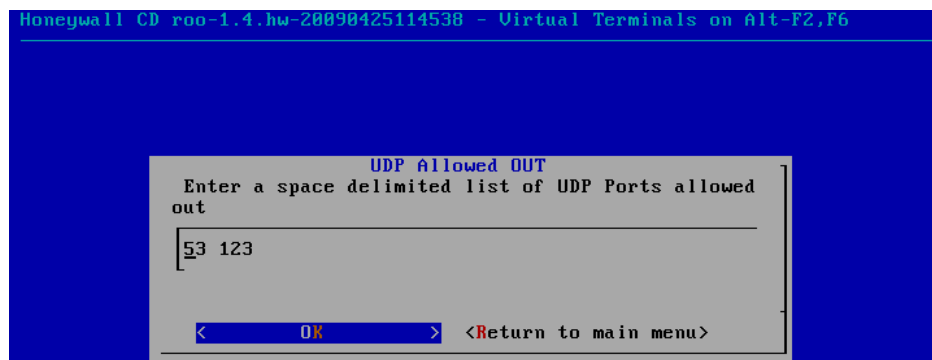


Gráfico A1 11 Puertos UPD escucha.

Posteriormente se establece los tiempos con los que se lleve el análisis, puede ser periódico o anual:

- Minutos.
- Horas
- Días
- Meses

### Snort Inline

Es una versión modificada de Snort, permitiendo el acceso a paquetes del iptables, creando una serie de listas para poder acceder o restringir.

Acceso no permitido

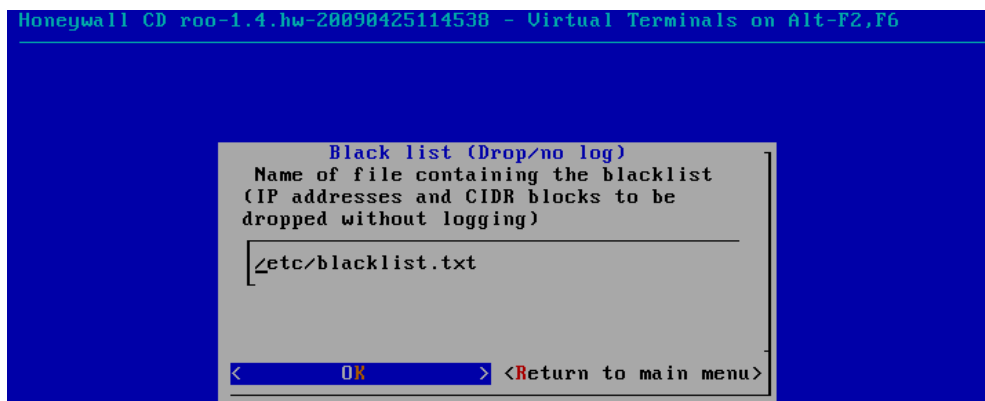


Gráfico A1 12 Listas no permitidas.

Acceso permitido

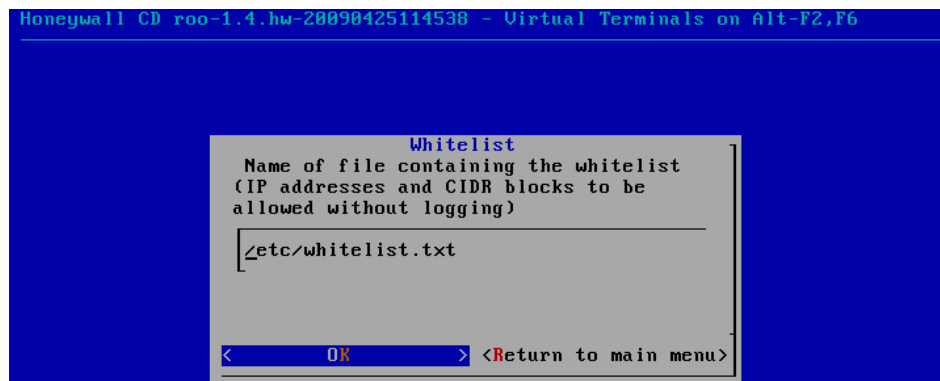


Gráfico A1 13 Listas permitidas.

Una vez finalizado todo, tendremos que corroborar la configuración en los documentos de Honeywall, para toda configuración se almacena un copia para no perder nada de información.

Sebek

Herramienta perteneciente a “The Honeynet PROJECT”, aquí configuramos el Servidor dentro del Honeywall, el cliente se configura el Honeypot o una terminal localizable en la red.

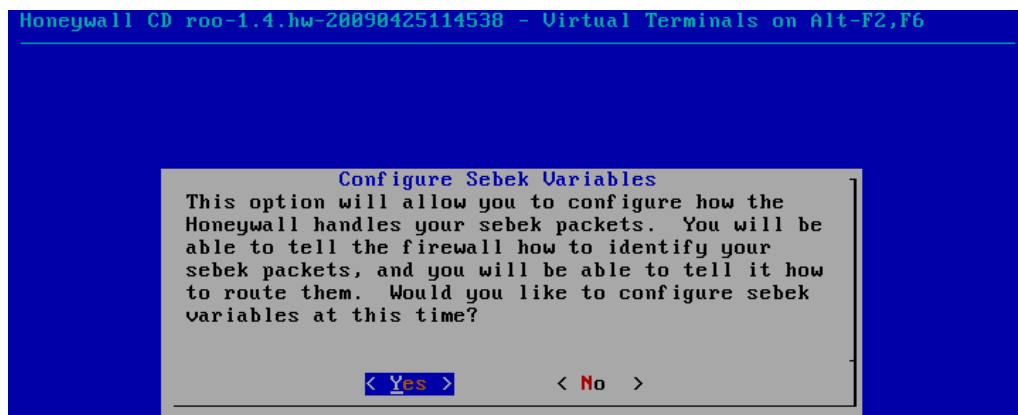


Gráfico A1 14 Configuración del SEBEK

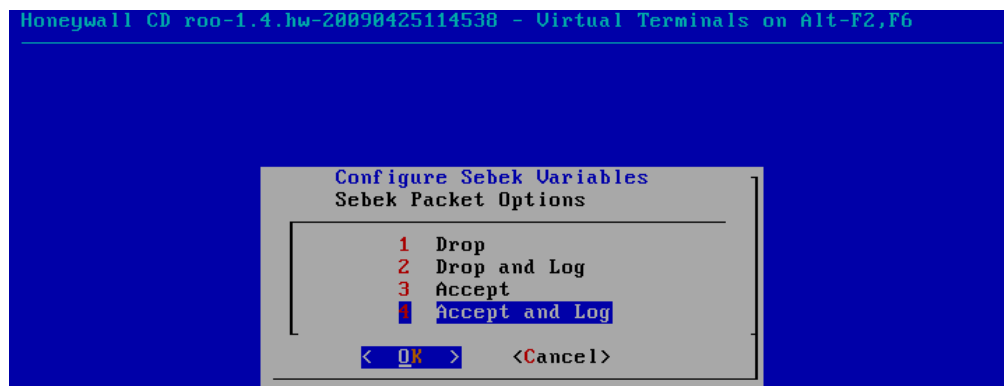


Gráfico A1 15 Método de acceso.

Una vez concluido toda la configuración del Honeywall podemos revisar los log generados en el Servidor “/var/log”.

## ANEXO A2

### Configuración de los servicios en CentOS 6.5

Virtualización utilizando el software VirtualBox.

En un Servidor físico normalmente se configuran servicios básicos como lo son nombres de domino, Servidor de base de datos y Servidor web.

#### **Información del Sistema:**

```
[root@serv ~]# uname -a #Información del SO
```

```
Linux serv 2.6.32-358.23.2.el6.i686 #1 SMP Wed Oct 16 17:21:31 UTC 2013 i686 i686  
i386 GNU/Linux
```

```
[root@serv ~]# fdisk -l #Información de las particiones
```

```
Disk /dev/sda: 8589 MB, 8589934592 bytes  
255 heads, 63 sectors/track, 1044 cylinders  
Units = cylinders of 16065 * 512 = 8225280 bytes  
Sector size (logical/physical): 512 bytes / 512 bytes  
I/O size (minimum/optimal): 512 bytes / 512 bytes  
Disk identifier: 0x0001a53b
```

Device	Boot	Start	End	Blocks	Id	System
/dev/sda1	*	1	64	512000	83	Linux

Partition 1 does not end on cylinder boundary.

/dev/sda2		64	1045	7875584	8e	Linux LVM
-----------	--	----	------	---------	----	-----------

```
Disk /dev/mapper/VolGroup-lv_root: 5947 MB, 5947523072 bytes
```

255 heads, 63 sectors/track, 723 cylinders  
Units = cylinders of 16065 \* 512 = 8225280 bytes  
Sector size (logical/physical): 512 bytes / 512 bytes  
I/O size (minimum/optimal): 512 bytes / 512 bytes  
Disk identifier: 0x00000000

Disk /dev/mapper/VolGroup-lv\_swap: 2113 MB, 2113929216 bytes  
255 heads, 63 sectors/track, 257 cylinders  
Units = cylinders of 16065 \* 512 = 8225280 bytes  
Sector size (logical/physical): 512 bytes / 512 bytes  
I/O size (minimum/optimal): 512 bytes / 512 bytes  
Disk identifier: 0x00000000

[root@serv ~]# free -m **#Información de memoria RAM total y ejecución**

	total	used	free	shared	buffers	cached
Mem:	499	466	32	0	48	176
-/+ buffers/cache:		241	257			
Swap:	2015	0	2015			

[root@serv ~]# w **#Usuarios del sistema**

11:08:22 up 2:42, 5 users, load average: 1.38, 1.51, 1.44

USER	TTY	FROM	LOGIN@	IDLE	JCPU	PCPU	WHAT
root	tty7	:1	11:04	2:42m	3.67s	3.67s	/usr/bin/Xorg :
root	pts/1	:1.0	11:04	3:49	0.00s	0.00s	bash
root	pts/2	:1.0	11:04	0.00s	0.06s	0.00s	w



## **Configuraciones generales del Sistema**

### **Tarjetas de red:**

```
[root@serv ~]# ifconfig
eth4  Link encap:Ethernet HWaddr 08:00:27:05:B9:EE
      inet addr:192.168.1.10 Bcast:192.168.1.255 Mask:255.255.255.0
      inet6 addr: fe80::a00:27ff:fe05:b9ee/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:3366 errors:0 dropped:0 overruns:0 frame:0
      TX packets:4693 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:3946832 (3.7 MiB) TX bytes:280764 (274.1 KiB)
```

### **Archivo de configuración para resolver nombres del dominio:**

```
[root@serv ~]# more /etc/resolv.conf
# Generated by NetworkManager
nameserver 192.168.1.10
```

### **Resoluciones que requiera el Host (maquina o SO):**

```
[root@serv ~]# more /etc/host.conf
multi on
order hosts,bind
```

### **Direcciones de los hosts del Servidor:**

```
[root@serv ~]# more /etc/hosts
```

```
#127.0.0.1 localhost4.localdomain4 localhost4
#::1 localhost6.localdomain6 localhost6
192.168.1.10 serv.fishoney.com serv
```

## Servicios levantados

### DNS

Servicio de nombres de dominio:

```
[root@serv ~]# more /etc/named.conf
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//

options {
    listen-on port 53 { 192.168.1.10; };
    #listen-on-v6 port 53 { fec0::a00:27ff:fea8:c91f; };
    directory "/var/named";
    dump-file "/var/named/data/cache_dump.db";
    statistics-file "/var/named/data/named_stats.txt";
    memstatistics-file "/var/named/data/named_mem_stats.txt";
    #allow-transfer { localhost; 192.168.1.10; };
    allow-query { any; };
    recursion yes;

    dnssec-enable yes;
    dnssec-validation yes;
    dnssec-lookaside auto;

    /* Path to ISC DLV key */
    bindkeys-file "/etc/named.iscdlv.key";

    managed-keys-directory "/var/named/dynamic";
};

logging {
    channel default_debug {
```

```

        file "data/named.run";
        severity dynamic;
    };
};

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

zone "fishoney.com" IN {
    type master;
    file "directo.zone";
    allow-update { none; };
    #allow-transfer { 192.168.1.10; };
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";

```

```

[root@serv ~]# more /var/named/chroot/var/named/directo.zone
$TTL 1D
@      IN SOA      serv.fishoney.com. root.serv.fishoney.com. (
                                0      ; serial
                                1D     ; refresh
                                1H     ; retry
                                1W     ; expire
                                3H )   ; minimum
      IN  NS     serv.fishoney.com.
serv   IN  A     192.168.1.10
www    IN  A     192.168.1.10

```

## WEB

Servicio para módulos web:

```
[root@serv ~]# more /etc/httpd/conf/httpd.conf
```

```

#
# This is the main Apache server configuration file. It contains the
# configuration directives that give the server its instructions.
# See <URL:http://httpd.apache.org/docs/2.2/> for detailed information.
# In particular, see

```

```
# <URL:http://httpd.apache.org/docs/2.2/mod/directives.html>
# for a discussion of each configuration directive.
#
```

```
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, in addition to the default. See also the <VirtualHost>
# directive.
```

```
Listen *:80
```

```
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
```

```
ServerName 192.168.1.10:80
```

```
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#
```

```
DocumentRoot "/var/www/html"
```

```
#
# This should be changed to whatever you set DocumentRoot to.
#
<Directory "/var/www/html">
```

```
#
# Use name-based virtual hosting.
#
NameVirtualHost *:443
```

### **Base de datos**

Servicio o Servidor de base de datos, POSTGRESQL:

```
[root@serv ~]# more /var/lib/pgsql/9.1/data/pg_hba.conf
```

```
# TYPE DATABASE USER ADDRESS METHOD
```

```
# "local" is for Unix domain socket connections only
local all all peer
```

```

# IPv4 local connections:
#host all all 127.0.0.1/32 ident
# IPv6 local connections:
host all all ::1/128 ident
# Allow replication connections from localhost, by a user with the
# replication privilege.
#local replication postgres peer
#host replication postgres 127.0.0.1/32 ident
#host replication postgres ::1/128 ident
host all all 192.168.1.0/24 md5
host all all 172.0.0.1/32 md5

```

## Servicios en ejecución

```

[root@serv ~]# service named restart
Stopping named: . [ OK ]
Starting named: [ OK ]
[root@serv ~]# service httpd restart
Stopping httpd: [ OK ]
Starting httpd: [ OK ]
[root@serv ~]# service postgresql-9.1 restart
Stopping postgresql-9.1 service: [ OK ]
Starting postgresql-9.1 service: [ OK ]
[root@serv ~]# █

```

Gráfico A2 Servicios en ejecución 1