Universidad Austral de Chile

Facultad de Ciencias de la Ingeniería
Escuela de Ingeniería Civil en Informática

“ICIHONEY: Diseño e Implementación de una Red Trampa en el Instituto de Informática de la Universidad Austral de Chile"

Tesis para optar al Título de
Ingeniero Civil en Informática

Profesor Patrocinante:
Sr. Luís Hernán Vidal Vidal
Ingeniero Civil en Informática

Co-Patrocinante:
Sr. Daniel Eugenin Morales
Ingeniero Civil en Informática.

Profesor Informante:
Sr. Christian A. Lazo Ramírez
Técnico Electromecánico
Ingeniero Gestión Informática
Diploma de Estudios Avanzados, Ingeniería Telemática.
Doctor en Ingeniería Telemática

JORGE WALDEMAR TRAPP FLORES

Valdivia – Chile
2009

Universidad Austral de Chile

Instituto de Informática

Valdivia, 9 de Abril de 2009.

De : Luis Hernán Vidal Vidal.
A : Sr. Juan Pablo Salazar F.
Director de Escuela de Ingeniería Civil en Informática.
Ref. : Informa Calificación Trabajo de Titulación.

MOTIVO: Informar revisión y calificación del Proyecto de Título "ICIHONEY: Diseño e Implementación de una Red Trampa en el Instituto de Informática de la Universidad Austral de Chile", presentado por el alumno JORGE WALDEMAR TRAPP FLORES, que refleja lo siguiente:

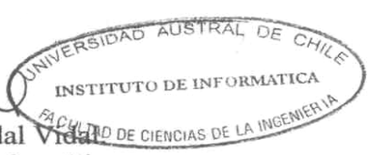
Se logró el objetivo planteado que permitió diseñar e implementar un prototipo de red trampa en el Instituto de Informática de la Universidad Austral de Chile, la cual permitirá analizar, controlar y monitorear la red ante posibles ataques tanto internos como externos.

El esfuerzo constante, junto con la dedicación al tema son aspectos destacables durante el proceso del trabajo realizado.

Cumplimiento del objetivo propuesto.	7,0
Satisfacción de alguna necesidad.	7,0
Aplicación del método científico.	7,0
Interpretación de los datos y obtención de conclusiones.	7,0
Originalidad.	7,0
Aplicación de criterios de análisis y diseño.	7,0
Perspectivas del trabajo.	7,0
Coherencia y rigurosidad lógica.	7,0
Precisión del lenguaje técnico en la exposición, composición, redacción e ilustración.	7,0
Evaluación Tesis.	**7,0**

Por todo lo anterior expuesto califico el trabajo de titulación del Sr. JORGE WALDEMAR TRAPP FLORES con nota 7,0 (seis coma nueve).

Sin otro particular, se despide atentamente.



Ing. Luis Hernán Vidal Vidal.
Profesor Instituto de Informática.
Facultad de Ciencias de la Ingeniería.
Universidad Austral de Chile.

Santiago, 17 de Abril de 2009

Sr. Juan Pablo Salazar Fernández
Director de Escuela Ingeniería Civil en Informática
Universidad Austral de Chile

De mi consideración,

El motivo de la presente es para informar a Ud. la calificación del siguiente Trabajo de Titulación:

Título:
"ICIHONEY: DISEÑO E IMPLEMENTACIÓN DE UNA RED TRAMPA EN EL INSTITUTO DE INFORMÁTICA DE LA UNIVERSIDAD AUSTRAL DE CHILE"

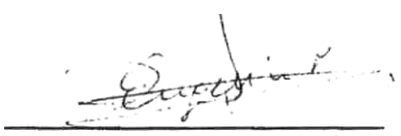
Nombre del Alumno:
Sr. Jorge Waldemar Trapp Flores

La estructura de la Tesis desarrollada por el Sr. Trapp permite comprender claramente los objetivos de su trabajo, cómo éstos han sido logrados, y de qué manera aporta su trabajo dentro del área en que se encuentra inmerso. El trabajo se apoya en una excelente base teórica para dar a conocer términos importantes que se aplicarán durante su desarrollo, y su implementación demuestra las capacidades de integración de tecnologías adecuadas para dar una solución propuesta al problema planteado. Sin embargo, considero demasiado extenso el anexo acerca de la instalación y configuración de equipos como también el resultado de los reportes de vulnerabilidades, los cuales debería resumir e interpretar, respectivamente.

Se analizaron diversos factores, de acuerdo a la siguiente tabla:

Item	Nota
Cumplimiento del objetivo propuesto	7,0
Satisfacción de alguna necesidad	7,0
Aplicación del método científico	7,0
Interpretación de los datos y obtención de conclusiones	G,0
Originalidad	7,0
Aplicación de criterios de análisis y diseño	7,0
Perspectivas del trabajo	7,0
Coherencia y rigurosidad lógica	7,0
Precisión del lenguaje técnico en la exposición, composición, redacción e ilustración	6,5
NOTA FINAL	**6,8**
En palabras:	Seis coma Och

Sin otro particular, saluda atentamente a usted



Daniel Antonio Eugenín Morales
Co-Patrocinante
13.756.988-4

Valdivia, 28 de Abril de 2009

De: Christian Lazo Ramírez
Profesor Informante

A: Juan Pablo Salazar Fernández
Director
Escuela de Ingeniería Civil en Informática

Ref: Calificación proyecto de título

De mi consideración:

Habiendo revisado el trabajo de titulación "**ICIHONEY: Diseño e Implementación de una Red Trampa en el Instituto de Informática de la Universidad Austral de Chile",** presentado por el alumno sr. **JORGE WALDEMAR TRAPP FLORES,** mi evaluación del mismo es la siguiente:

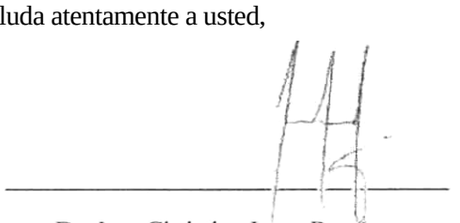
Nota: 6,5 (SEIS COMA CINCO).

Fundamento de la nota:

El trabajo de título realizado por el alumno cumple a cabalidad con los objetivos planteados, con una presentación y desarrollo del tema muy adecuado y contingente, ya que es parte de un área de la ingeniería que esta en constante evolución desde el punto de vista científico-tecnológico. Finalmente entrega conclusiones acertadas lo que demuestra una madurez del conocimiento alcanzado y de la situación estudiada.

Aspecto	**Evaluación**
Cumplimiento de objetivos	7,0
Satisfacción de alguna necesidad	6,5
Aplicación del método científico	6,5
Interpretación de los datos y obtención de conclusiones	6,4
Originalidad	6,6
Aplicación de criterios de análisis y diseño	6,5
Perspectivas del trabajo	6,0
Coherencia y rigurosidad lógica	6,3
Precisión del lenguaje técnico	6,4

Sin otro particular, saluda atentamente a usted,



Dr. Ing. Christian Lazo Ramírez
Académico
Instituto de Informática

Cuando lo creas todo perdido, no olvides que aún te queda el futuro,

tu cerebro, tu voluntad y dos manos para cambiar tu destino.

Wernher von Braun

Dedicada a

Don Waldemar Trapp Arias

AGRADECIMIENTOS

En primer lugar agradecer a Dios, por permitirme culminar una nueva etapa en mi vida, gozar de buena salud y tener una hermosa familia.

Agradecer también a mis papás y hermana por hacer de mi lo que soy, ya que todo lo que tengo y todo lo que he obtenido es gracias a su amor, esfuerzo y apoyo incondicional.

A mi Kozita por su amor, cariño, motivación para culminar este gran paso y por estar siempre a mi lado.

A toda mi familia por estar presente en todos los grandes pasos que he podido dar.

A los funcionarios del Instituto como Carlitos, Sra. Juanita, Verito, Marianne, Erwin y Jorge Cid por estar siempre dispuestos a ayudar. También a los Guardias del Campus Miraflores como: Pedro Henríquez, Félix Jaramillo, Osvaldo Jaramillo, Hugo López, José Pérez, Iván Rivera, Nolberto Sanzana y Domingo Torres porque sin ellos no hubiera podido finalizar esta tesis.

A todos los compañeros de Universidad los cuales dejan un lindo recuerdo de los momentos compartidos, en especial: Oscar, José, Kenneth, Chiqui, Callo, Zillo, Andrew, Chozo, Raúl, Seba, Rodolfo, Quezada, Lidia, Edgardo, Anita, Cristian, Aníbal, Humberto, Feña, Ramiro, Peralta, Livio, Mónica, Shepu, Pipo, Chamaco, Salas, Frankie, Karina, Carmen, Gori, Pato, Gerardo, Dumont, Manolo, Karen, Barby, Jonny, Kyo, Edison, Castillo, Waleska, Tatiana, Sioux, Dainerys, Roberto, Sitnisky, Anto, Naty, Poshoclo, Valeria, Maykel, Pancho, Lillo, Mauri, Sergio, Xime, Deisy, Patana y todos aquellos con los pude compartir durante el paso por esta Universidad.

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Este proyecto de titulación consiste en diseñar e implementar una Honeynet en el Instituto de Informática de la Universidad Austral de Chile. Para ello, se debe investigar todo lo relacionado con Seguridad Informática a fin de entender donde se encuentra inmerso el proyecto y comprender como se ha administrado la red del Instituto para poder realizar un completo análisis y diseño de la Honeynet más adecuada a ésta.

Una vez analizada la red e investigado lo relacionado con Seguridad Informática se diseña un prototipo de Honeynet acorde a la red del Instituto tomando en cuenta la topología de ésta y los recursos disponibles.

El desarrollo de este prototipo implica comprender las distintas técnicas de Seguridad Informática utilizadas por los Intrusos para vulnerar sistemas, junto con instruirse en mejorar la configuración de los equipos.

El prototipo fue implementado en el laboratorio de Tesistas del Instituto de Informática, donde se encuentra funcionando correctamente, permitiendo un aumento en la seguridad y un mayor control de los equipos configurados.

Para la implementación se tomó en cuenta los equipos que estaban disponibles y de acuerdo a sus características se eligieron los sistemas operativos para obtener un funcionamiento óptimo de estos.

La evaluación de este proyecto consiste en realizar un ataque al sistema tomando en cuenta las acciones típicas de un atacante. Esto, permite conocer las respuestas generadas por el sistema y los dos puntos de vista más importantes: del atacante y del administrador del sistema.

ABSTRACT

The following Thesis Project consists on designing and implementing a Honeynet in the Informatics Institute at the Austral University of Chile. In this way, it must be investigate everything related with Informatics Security to understand where this project is aimed and the way the Institute Net has been administrated so that to make a complete analysis and design of the most accurate Honeynet.

Once the net is analyzed and the Informatics Security investigated, the project introduces a Honeynet model related to the net the institute has, considering its topology and available resources.

The development of this model means to understand the different informatics security techniques used by the hackers to violate the systems; together with getting information for improving the equipment configuration.

The model was created and implemented in the Thesis Laboratory in the Informatics Institute, where it is working nowadays in an accurate way, allowing an increase in the security system and giving a better control of the configured equipments.

In order to implement the project, it was considered the available equipment, and according to its characteristics was chosen the Operating Systems so as to get the best functioning of them.

The evaluation of this project consists in making a system attack considering the typical hacker actions. This, to permit recognizes the responses generated by the system and the two key viewpoints most important: the attacker and the system administrator.

Capítulo I INTRODUCCIÓN

1.1 Antecedentes Generales

Internet se ha transformado en los últimos años en el nuevo santo grial de la civilización, términos que hasta hace algunos años no se conocían, ahora son comúnmente utilizados. Tal es el crecimiento de Internet que al 30 de Junio de 2008 hay más de 1400 millones de personas conectadas a Internet [INT08] así como 570 millones de sitios Web en Julio de 2008 [ISC08].

El impacto tecnológico que ha generado Internet en la sociedad ha sido tan grande que ha trascendido la propia red y es muy difícil no encontrar referencias casi a diario en otros medios de comunicación tales como televisión, prensa, radio, etc. Para ver hasta qué punto Internet está absorbiendo los medios de comunicación tradicionales, sólo cabe destacar cómo la mayor parte de diarios importantes del mundo tienen sus símiles en edición digital, los cuales son consultados diariamente por millones de usuarios.

Las organizaciones únicamente digitales tales como Google, Yahoo, etc., cada vez toman una mayor relevancia y un considerable peso económico, esto se puede observar en cómo están presentes en los mercados bursátiles y cómo mueven cientos de millones de dólares de igual forma que lo realizan otras organizaciones más tradicionales.

Para cualquier organización que tenga la Informática o Internet como estructura fundamental de su funcionamiento, el tema de la seguridad es sin duda de gran relevancia debido a que tanto la disponibilidad como la confiabilidad de la información son un tema crítico dentro de la organización. Saber identificar los posibles riesgos a los que se pueda ver expuesta dicha información es imprescindible para asegurar la integridad y el correcto uso que a ésta se le puede dar.

La gran variedad de protocolos, tecnologías y servicios que sustentan Internet hacen que la posibilidad de realizar un ataque sea muy elevada, debido a que el concepto de seguridad no fue un elemento primordial del diseño inicial de Internet.

Con los datos de utilización de Internet anteriormente descritos, se puede observar que si tan sólo el 1 por ciento de la población realiza ataques mediante la red, se tiene que existen casi 14 millones de posibles atacantes.

En las estadísticas anuales de organismos oficiales como el CERT[1] que se encarga de monitorear y analizar las vulnerabilidades de seguridad en Internet [CER08], se puede observar cómo se ha incrementado la cantidad de incidentes registrados año a año. Este incremento ha venido de la mano con una evolución de las técnicas y herramientas utilizadas por los atacantes. Aún cuando el aumento se ha ido estancando sigue siendo relativamente elevado. Esto se puede apreciar más claramente en la Figura Nº1 que se muestra a continuación.

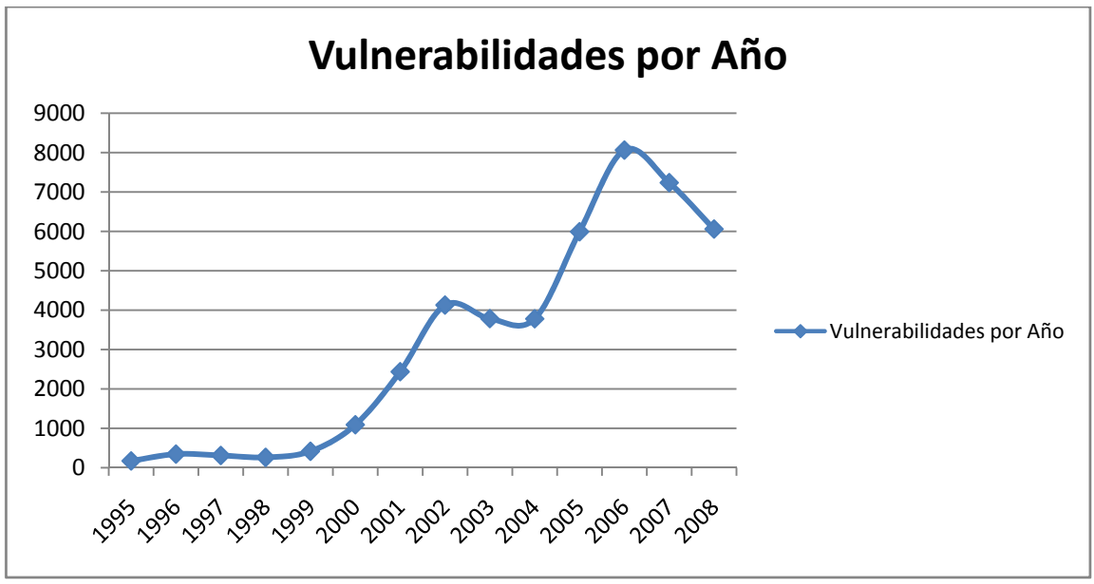


Figura Nº 1 Aumento de Vulnerabilidades. Fuente: CERT

Por bastante tiempo, la Seguridad Informática ha sido meramente defensiva. Ésta consistía principalmente en defender la infraestructura de la información, detectar fallos y reaccionar a estos. Con el cambio que está surgiendo en Internet el cual se debe principalmente al gran avance tecnológico y a la evolución de las técnicas de los atacantes, se requiere un nuevo modelo que permita ampliar el concepto de seguridad.

Dentro de este nuevo modelo aparece el concepto de pro-actividad dentro de la Seguridad Informática, en el cual no se dejan de lado herramientas antes utilizadas, sino que junto a éstas aparecen nuevas técnicas que permiten detectar e incluso prevenir nuevos ataques.

Una de estas nuevas técnicas es el *Sinkhole* o sumidero, la cual consiste en eliminar el tráfico sospechoso de la red. Además, mediante el uso de señuelos se puede obtener información valiosa sobre las amenazas, las cuales pueden ser observadas, analizadas y monitorizadas previniendo nuevos ataques. El *Sinkhole* lo utilizan principalmente los

[1] Computer Emergency Response Team http://www.cert.org

proveedores de Internet, lo que al sumarle señuelos produce una interesante aplicación, ya que el tráfico malintencionado, no sólo se elimina, sino que permite realizar estudios, los que a su vez permiten identificar cuáles son las técnicas utilizadas en los ataques.

Dentro de esta nueva forma de ver la seguridad, aparecen los *Honeypots* o "potes de miel". Éstos, pretenden conocer al enemigo, conocer sus técnicas y formas de actuar. En los capítulos siguientes se explica exhaustivamente en qué consisten, centrándose principalmente en las *Honeynets* (redes de miel) y cómo éstas permiten un completo estudio de los atacantes.

Este proyecto consiste en diseñar e implementar un prototipo de Honeynet en la red del Instituto de Informática de la Universidad Austral de Chile, la cual permitirá mejorar considerablemente el nivel de seguridad presente en la red del Instituto. Además, permitirá utilizar los datos obtenidos como herramienta de investigación y aprendizaje tanto para los alumnos como profesores de la carrera Ingeniería Civil en Informática de la Universidad.

1.2 Contribución de la Tesis

La motivación de este proyecto nace a partir de la necesidad de profundizar temas de seguridad en redes y llevarlos a la práctica para mejorar la seguridad de la red del Instituto de Informática, lo que permitirá estar a la vanguardia de la innovación nacional. La idea es que la red del Instituto sea más segura en un sentido pro-activo, esto significa adelantarse al enemigo, conociendo su forma de actuar y así poder anticipar sus ataques. Por este motivo, se hace necesario implementar medidas de seguridad en la red del Instituto que permitan prevenir un posible ataque.

El desafío principal de este proyecto será enfocarlo con fines educativos de manera de entregar un aprendizaje práctico no sólo a los estudiantes de la asignatura de Redes, sino que, incluir a todos los estudiantes de la carrera Ingeniería Civil en Informática de la Universidad Austral de Chile.

1.3 Impactos

El desarrollo de este proyecto generará un impacto a todos los alumnos y docentes del Instituto de Informática de la Universidad Austral de Chile debido a que sus equipos se verán hasta cierto punto más protegidos frente a ataques de algún malintencionado. El conocimiento de nuevas formas de Seguridad que adquirirán alumnos y docentes, posicionará tanto al Instituto como a la Universidad a la vanguardia en Seguridad Informática a nivel nacional.

Además, no generará un gran volumen de datos lo que permitirá un tráfico expedito de la red. Sin embargo, los datos generados serán de altísimo valor para el análisis y monitorización de la red. Por esto, éste prototipo trae consigo una red más prevenida y segura frente a posibles ataques, por ende equipos más seguros y estables.

1.4 Objetivos Generales

Diseñar e Implementar un prototipo de Red Trampa en el Instituto de Informática de la Universidad Austral de Chile, la cual permitirá analizar, controlar y monitorear la red ante posibles ataques tanto internos como externos.

1.5 Objetivos Específicos

- Identificar y Describir las tecnologías honeypot y honeynet como herramientas de seguridad y la forma en que afectan el actual funcionamiento de la red del Instituto de Informática.
- Diseñar una Red Trampa adecuada a la realidad del Instituto de Informática.
- Implementar un prototipo funcional de Red Trampa que permita proteger, analizar y monitorear la red del Instituto de Informática en un ambiente real.
- Evaluar las diferencias reflejadas por la incorporación de la Red Trampa en la red del Instituto de Informática.

1.6 Organización de la Tesis

Esta tesis está estructurada por 7 capítulos, los cuales están organizados de la siguiente forma:

Capítulo I Introducción: En este capítulo, se describe el contexto en el cual está inmerso el proyecto, el alcance, motivación e impactos de éste, junto con la nomenclatura a utilizar en su desarrollo.

Capítulo II Seguridad Informática: En este capítulo, se describe la Seguridad Informática y como se aplica en distintos ámbitos. Además, se explica el marco legal vigente en el País y se presentan los tipos de intrusos que afectan la seguridad de los sistemas informáticos, sus diferencias y formas de actuar.

Capítulo III *Honeypot*/*Honeynet*: En este capítulo se detallan las tecnologías Honeypot y Honeynet, sus características, ventajas y desventajas, así como también algunas variantes que han sufrido al complementarse con otras tecnologías como los Wireless Honeypot, Honeynet Virtuales y las Honeynet distribuidas.

Capítulo IV Desarrollo: En este capítulo, se describe y analiza la red del Instituto de Informática, junto con el diseño de una Honeynet acorde a ésta. Posteriormente, se enseña la implementación y evaluación de la Honeynet en la red del Instituto, visto desde la perspectiva del atacante y del administrador del sistema.

Capítulo V Conclusiones y Trabajos Futuros: En este capítulo, se comentan los resultados obtenidos, junto con dar a conocer las conclusiones obtenidas de la implementación de la Honeynet en el Instituto de Informática. Además, se plantean posibles mejoras al sistema y trabajos futuros.

Capítulo VI Referencias Bibliográficas: En este capítulo, aparecen las referencias bibliográficas citadas en el documento de tesis.

Capítulo VII Anexos: En este capítulo, aparece la ley chilena relativa a los delitos informáticos, las instalaciones y configuraciones de los equipos y los reportes de vulnerabilidades generados por las herramientas utilizadas para esta función.

1.7 Nomenclatura

En el desarrollo de la tesis, aparecen términos en idiomas distintos al español, muchos de los cuales no se traducen debido a que son de uso frecuente en Informática, o debido a que es más complejo utilizar un término apropiado en español o simplemente no tienen una traducción a este idioma. Por este motivo, se escriben en su idioma original con formato de fuente *cursiva.*

En general, se trabaja con un máximo de 3 niveles de profundidad de información. Las definiciones tendrán una sangría de 1.2 cms. por la izquierda y de 1.8 cms. por la derecha, excepto en el caso que se utilicen viñetas, en cuyo caso, la viñeta también estará a 1.2 cms. por la izquierda, pero no tendrá sangría por la derecha.

Capítulo II SEGURIDAD INFORMÁTICA

2.1 Introducción

El amplio desarrollo de nuevas tecnologías informáticas y el aumento de velocidad de las redes, brindan un nuevo campo de acción a los antisociales para llevar a cabo sus ataques, como accesos no autorizados o robo de información crítica. Con la proliferación de amenazas cada vez más sofisticadas, la seguridad de la información se ha tornado cada vez más importante, incluso más allá de la simple identificación de las amenazas, vulnerabilidades e intrusiones.

Los primeros conceptos de seguridad se remontan a los comienzos de la escritura con los Sumerios (3000 AC). A su vez, la Biblia, escritores griegos y romanos presentan en sus escrituras rasgos de seguridad en la guerra y el gobierno. Por esto, la seguridad no es un concepto nuevo, sino que ha ido acompañando al hombre desde tiempos remotos.

2.1.1 ¿Qué es Seguridad?

"Libre y exento de todo peligro, daño o riesgo".[2]

> "Seguridad es una necesidad básica. Estando interesada con la preservación de la vida y las posesiones, es tan antigua como la vida.". [MAN]

Sin duda los descubrimientos arqueológicos son las pruebas más importantes de seguridad en la antigüedad. Los primitivos utilizaban métodos defensivos de los animales, las civilizaciones antiguas creaban templos, palacios o pirámides para almacenar sus posesiones.

La Seguridad Moderna tiene su origen en la revolución industrial con el fin de combatir los delitos y movimientos laborales de la época. Henry Fayol en 1919 define el objetivo de la seguridad como "salvaguardar propiedades y personas contra el robo, fuego e inundación, contrarrestar huelgas y felonías, y todos los disturbios sociales que puedan poner en peligro el progreso e incluso la vida del negocio". Con esto, se puede ver que Fayol solo hace referencia a cosas materiales ya que en esa fecha las cosas materiales eran lo más importante.

[2] Definición de seguro/ra. Real Academia Española http://www.rae.es

La primera definición general del término seguridad de sistemas informáticos la dan Garfinkel y Spafford [GAR91] como aquello de lo que se puede depender para que se comporte como se espera. Un sistema es seguro desde el punto vista de un usuario si la serie de acciones que cada actor puede realizar están limitados por lo que el usuario cree que el actor puede hacer [KUM95].

Una definición más exhaustiva de lo que hoy conocemos como Seguridad Informática está basada en la obtención de confidencialidad, integridad y disponibilidad en un sistema informático [PFL97].

2.1.2 Objetivo de la Seguridad Informática

> "El objetivo de la Seguridad Informática es mantener la Integridad, Disponibilidad, Privacidad, Control y Autenticidad de la información manejada por computador" [ALD98].

Donde Información "es una agregación de datos que tiene un significado específico más allá de cada uno de éstos" [FER08]. Cuyas principales características son: ser crítica, valiosa y sensitiva.

Crítica: es necesaria para certificar la persistencia operativa.

Valiosa: es un activo con valor propio.

Sensitiva: debe ser conocida solo por las personas que la procesan.

La Integridad de la Información: se refiere a la característica que mantiene el contenido de la información para que éste no sea alterado, excepto que sea modificado por personal autorizado.

La Disponibilidad de la Información: es la capacidad de estar persistentemente utilizable para ser procesada por personal autorizado.

La Privacidad de la Información: se refiere a la necesidad de que la información sea de carácter confidencial, esto es, sólo conocida por el personal autorizado.

El Control de la Información: se refiere a asegurar el acceso a la información sólo al personal autorizado.

La Autenticidad de la Información: se refiere a definir que la información utilizada es válida, pudiendo asegurar el origen de esta.

Se puede entender como Seguridad Informática entonces, como un estado el cual indica que un sistema está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar su correcto funcionamiento o los resultados que se obtienen del mismo. Este peligro, daño o riesgo, es lo que se define como amenaza. Estas amenazas pueden analizarse en tres momentos particulares, ya sea antes, durante y después del ataque.

> **Prevención:** La prevención es el análisis antes que se realice un ataque por medio de mecanismos que aumentan la seguridad de un sistema.
>
> **Detección:** La detección es el proceso que permite actuar durante el ataque mediante mecanismos de auditoría que permiten descubrir violaciones de seguridad.
>
> **Recuperación:** La recuperación es el proceso posterior a la agresión que mediante componentes de respaldo o *backup*, permiten volver al funcionamiento normal del sistema.

El indicador de seguridad de un sistema informático se puede definir como el porcentaje de seguridad de un sistema, pero lograr un 100% de seguridad es muy difícil sino imposible según los especialistas. Por ello, se habla de un sistema fiable en vez de seguro. Donde Fiabilidad se define como “La Probabilidad de buen funcionamiento de algo”.[3]

2.1.3 Niveles de Seguridad Informática

El estándar más utilizado para este fin, es el TCSEC[4] Orange Book[5] desarrollado por el departamento de defensa de Estados Unidos. Consiste en aplicar la política de seguridad del departamento de defensa para mantener la confidencialidad de la información mediante distintos niveles de seguridad. Los niveles se enumeran desde el menor grado de seguridad al máximo, y cada nivel abarca todos los niveles anteriores. Estos niveles, han sido la base para el desarrollo de estándares europeos e internacionales.

> **Nivel D:** Sistemas que no cumplen con ninguna especificación de seguridad se encuentran en este nivel. Sistemas sin protección, con sistemas operativos inestables y sin autenticación o control de acceso. Un ejemplo en cuanto a sistema operativo podría ser DOS.

[3] Definición de fiabilidad. Real Academia Española http://www.rae.es
[4] Trusted Computer System Evaluation Criteria
[5] Department Of Defense. Orange Book. Library Nº S225, 771. EEUU. 1983. http://www.doe.gov

Nivel C1: En este subnivel se requiere tener identificación de usuarios, haciendo distinción entre el administrador y los usuarios del sistema. Además, requiere de control de acceso discrecional haciendo distinción entre usuarios y recursos.

Nivel C2: Este subnivel cuenta con características adicionales al anterior, tales como auditoria de accesos, restringir mucho más el acceso a ciertos archivos por parte del usuario, no sólo en base a permisos sino que incluyendo niveles de autorización.

Nivel B1: Este subnivel permite asignar una etiqueta con un nivel de seguridad jerárquico a cada objeto del sistema. Además, se establecen controles para limitar la propagación de accesos a los distintos objetos. Es decir, cada usuario tiene sus objetos asociados.

Nivel B2: Este subnivel consiste en una protección estructurada, esto es, etiquetar cada objeto de nivel superior con un objeto de nivel inferior por ser padre de él. Así, por ejemplo un disco duro será etiquetado por almacenar archivos de distintos usuarios.

Nivel B3: Este subnivel consiste en reforzar los dominios de seguridad con la instalación de hardware adicional. Además, cada usuario tiene asignado lugares y objetos a los que puede acceder solo por medio de una conexión segura.

Nivel A: Es el mayor nivel, incluye procesos de diseño, control y verificación para asegurar todos los procesos realizados por un usuario del sistema. Se debe proteger tanto software como hardware para evitar infiltraciones ante movimientos o traslados de los equipos.

2.1.4 Intrusos y la protección de la Información

Se llama Intruso a la persona que ingresa sin autorización a un sistema ya sea de forma deliberada o no.

Según Julio Ardita director de CybSec S.A.[6] y ex hacker argentino “Los tipos de intrusos se pueden caracterizar desde el punto de vista del nivel de conocimiento, formando una pirámide. Para llegar desde la base hasta el tope de la pirámide se tarda desde 4 a 6 años,

[6] CybSec Security Systems. http://www.cybsec.com

por el nivel de conocimiento que se requiere asimilar" La Figura Nº4 presenta un resumen de los distintos niveles de la pirámide.

Clase A: El 80%, ubicado en la base de la pirámide, son los nuevos intrusos que bajan programas y los prueban son los llamados *Script Kiddies* que se definirán más adelante.

Clase B: El 12% siguiente, son más peligrosos, saben compilar programas aunque no saben programar. Prueban programas, detectan sistemas operativos, testean vulnerabilidades e ingresan por ellas.

Clase C: Es el 5%, gente que sabe, conoce y define sus objetivos. A partir de ahí buscan todos los accesos remotos e intentan ingresar.

Clase D: El 3% restante, entran a determinados sistemas y buscan la información que necesitan.

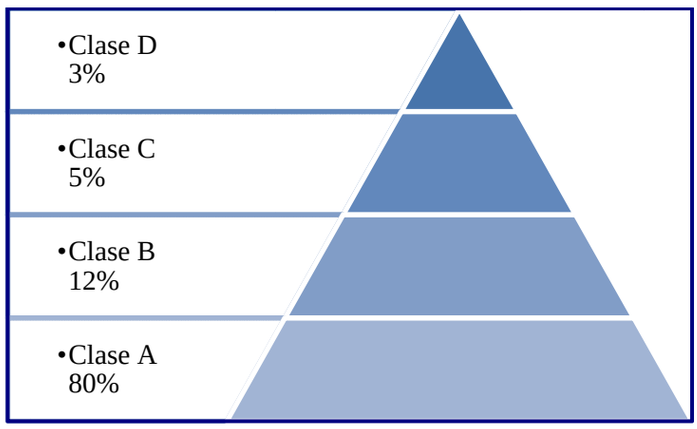


Figura Nº 2 Tipos de Intrusos. Fuente: CybSec S.A.

Para la protección de la información existen tres elementos básicos a proteger: hardware, software y datos.

Hardware es el conjunto de todos los sistemas físicos del sistema informático. Software son todos los elementos lógicos que permiten que el hardware sea funcional. Datos son el conjunto de información lógica que maneja el software y hardware.

De estos, los datos son los más importantes ya que son el resultado del trabajo realizado. Si fallara ya sea el hardware o el software se puede comprar nuevamente y remplazarlos, pero los datos son imposibles de reemplazar. Aun cuando se realicen copias de seguridad o *backup*, ya que es difícil restaurar los datos a su estado anterior.

2.2 Seguridad Física

Este último tiempo, se habla bastante de seguridad a nivel de red e Internet en una empresa, pero sin duda los equipos son mucho más vulnerables a los ataques físicos que a los ataques remotos. Porque sin duda, cuando alguien ataca a un servidor con un hacha los efectos posteriores son mucho más devastadores que un ataque remoto. Ya que si el equipo es atacado por red este se podrá reiniciar, reinstalar o reconfigurar, pero si el equipo fue dañado físicamente es mucho más grave.

La seguridad física entonces, consiste en la "Aplicación de barreras físicas, procedimientos de control y medidas de prevención ante amenazas a los recursos e información confidencial" [VIL02].

Por ello, es importante tratar este tema, donde algunos tópicos importantes son:

- Ubicación de los servidores y acceso físico a ellos (*Data Center*).
- Hardware de red.
- Contraseñas de equipos y control de acceso.
- Desastres naturales.

2.2.1 ¿Qué es un *Data Center*?

Un *Data Center* consiste en una sala equipada con piso anti-estático, climatizada, con circuitos inteligentes de manejo de energía, *backup* energético y acceso restringido con el fin de ubicar los servidores principales de una organización. Cuentan con presencia de personal técnico, servicio de vigilancia y control de acceso.

Para su realización existen normas, una de ellas y la principal es la norma EIA/TIA 942[7], esta norma se aplica a la infraestructura de telecomunicaciones estándar de *Data Center*, ingeniería de diseño, procedimientos, estándares técnicos que aseguran el funcionamiento óptimo de los fabricantes de productos asociados a la norma ISO 11801.

La norma ISO 11801[8] rige todos los procedimientos de instalaciones a nivel de corrientes débiles, define clases de aplicación y es denominado estándar de telecomunicaciones para edificios comerciales.

Los *Data Center* según la norma EIA/TIA 942 y su nivel de criticidad se pueden clasificar como lo muestra la Tabla Nº1.

[7] Telecommunications Infrastructure Standard for Data Centers http://www.tiaonline.org
[8] Information technology -- Generic cabling for customer premises http://www.iso.org

Tabla Nº 1 Cuadro de Criticidad de Data Center EIA/TIA 942

Nivel de Criticidad	*Data Center* / Proceso de Negocio	Infraestructura & Redundancia
C0	No es una propiedad crítica ni los procesos que ahí se ejecutan.	"Closet" en área de oficina, aire de confort, tiras de contactos protegidos.
C1	*Data Center* con nivel básico de criticidad, soporta procesos de oficina local no críticos. Perdida de servicio solo impacta a la productividad local.	Espacio dedicado, aire de confort o de precisión 24x7, UPS no redundantes, *sprinklers* húmedos.
C2	*Data Center* que soporta procesos de negocio críticos, locales y algunos remotos. Incluye *call centers*, algunas instalaciones de internet con servicios. Perdida de servicio afecta la productividad fuertemente dependiendo del horario.	UPS y HVAC múltiples (N). Capacidad de alimentación eléctrica de fuentes redundantes. Capacidad de *bypass* de mantenimiento, generador de respaldo, *sprinklers* secos y húmedos.
C3	Soporta una operación corporativa así como procesos de negocios críticos. La perdida de servicios afecta fuertemente la productividad y afecta directamente a algunos clientes.	UPS y HVAC N+1 o en algunos componentes 2N. Mantenimiento con aislamiento de carga y/o generador. Generación en N o N+1. *Sprinkles* secos y/o VESDA.
C4	Principal *Data Center* de la corporación operando todos los procesos de negocio. Perdida de servicio afecta de manera importante la productividad y afecta directamente a una gran parte de la base de clientes.	*Data Center* robusto y redundante. 2N en todos los componentes. No existe ningún punto único de falla.

2.2.2 Hardware de Red

La seguridad del hardware de red es otro tema de vital importancia, por ejemplo si un *router* de una empresa es colapsado puede provocar denegación de servicio a la empresa dejando toda la red inutilizada.

El riesgo de seguridad del hardware se debe principalmente a errores de parte del operador. Debido a la mala utilización de contraseñas de administración y a la mala configuración del hardware, lo que los hace vulnerables a posibles ataques.

2.2.3 Contraseñas de equipos y control de acceso

La mayoría de las arquitecturas de equipos utilizan contraseñas de BIOS-PROM, los fabricantes incluyen estos sistemas de contraseña para adherir una capa extra de seguridad a los equipos.

Las contraseñas de BIOS o de PROM evitan a los usuarios malintencionados acceder a la configuración del sistema. Sin embargo, no hay que olvidar que se debe establecer una contraseña de configuración o podría lamentarlo en el futuro. Aunque, se pueden anular estas contraseñas provocando un cortocircuito en la batería de la CMOS[9]. En algunos casos esto no es necesario ya que los fabricantes incluyen un jumper que permite borrar

[9] Complementary Metal Oxide Semiconductor

la CMOS. La CMOS es un conjunto de familias lógicas utilizadas en la fabricación de los chips computacionales.

El control de acceso es fundamental para mantener segura la información, desde una simple contraseña a sistemas biométricos para el ingreso a *Data Centers*. Estos últimos, permiten autenticar a los usuarios en base a características biológicas entre las que se incluyen: voz, iris o patrones de retina, huellas dactilares, estructura facial, olor corporal.

El control biométrico tiene sus pros y contras. Por un lado, ofrecen un alto grado de seguridad, sobre todo los sistemas que utilizan huellas digitales. Sin embargo, existen impedimentos prácticos para implantar un enfoque completamente biométrico. Ya sea por motivos de invasión de la privacidad, motivos sociales o por estar en lugares alejados (usuarios remotos). Pese a estos problemas, los controles de acceso biométricos son excelentes herramientas cuando se utilizan en lugares cerrados.

2.2.4 Desastres Naturales

El fuego es la principal amenaza contra la seguridad, siendo considerado el principal enemigo de los computadores. Los incendios generalmente son causados por fallas en instalaciones eléctricas, el uso inadecuado de combustibles y traslado de sustancias peligrosas. Los sistemas anti fuego existentes no generan certeza en cuanto a seguridad ya que resultan peligrosos para los empleados ya que se basan en dióxido de carbono.

Las inundaciones son la invasión de agua por el exceso o acumulación, ocasionada por la falta de drenaje. Además de las causas naturales, podría ocurrir una inundación provocada por un incendio en un piso superior.

Las tormentas, tempestades, tifones y terremotos, son catástrofes atmosféricas que dependen la probabilidad de ocurrencia y lugar del mundo donde se encuentre. Su frecuencia y ocurrencia se deben tener en cuenta, tomando precauciones adicionales ante la proximidad de una de estas catástrofes.

2.3 Seguridad Lógica

Seguridad Lógica es la aplicación de barreras que protejan el acceso a los datos y permitan el acceso sólo a personas autorizadas.

La idea es restringir el acceso al software y a los datos, asegurar que la utilización de estos sea correcta. Asegurar también, que la información recibida sea igual a la

transmitida, y esta última solo sea recibida por el destinatario al cual se le envió dicha información.

La autenticación consiste en la verificación por parte del sistema de la identificación del usuario. La Seguridad Informática se basa en la efectiva administración de los permisos de acceso y autenticación.

Las contraseñas o *passwords* son las más utilizadas para la autenticación de los usuarios, debido a su bajo costo de implementación. Éstas sirven en gran medida si no son palabras fáciles de deducir para un atacante. Siendo fácilmente evitable, si los usuarios aumentan la complejidad de las contraseñas, junto con incluir políticas o encriptación de contraseñas. Con lo cual, será mucho más complejo para el atacante descifrarlas.

2.3.1 Amenazas Lógicas

Para la identificación de las amenazas se requiere conocer los tipos de ataques, el tipo de acceso y los objetivos del atacante. Desde 1990 en adelante, se vienen registrando cada día una mayor cantidad de ataques informáticos, siendo estos cada vez más sofisticados y difíciles de rastrear.

En 1992 el DISA[10] realizó un estudio de 38.000 ataques a sitios gubernamentales, el resultado de este estudio entre los años 1992 y 1995 se refleja en la Figura Nº3.

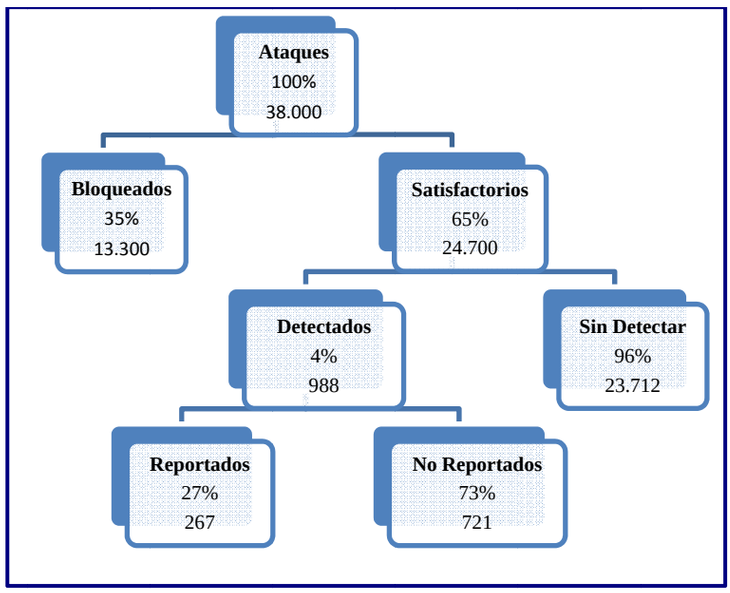


Figura Nº 3 Porcentaje de Ataques Fuente: www.disa.mil[11]

[10] DISA. Defense Information System Agency. http://www.disa.mil
[11] http://www.segu-info.com.ar/ataques/ataques.htm

Se puede ver que del total solo se reportaron 267 casos los que equivale al 0,7%. Esto, se debe principalmente, a que las empresas evitan reportar los incidentes ocurridos ya que estos bajarían el nivel de confianza de sus usuarios o clientes.

2.3.2 Elementos que permiten un Ataque

Si bien para algunas personas son calificados como tipos de ataques, en realidad son elementos que permiten lograr este fin, ya que gracias a estos es posible obtener información valiosa para poder vulnerar sistemas. Dentro de esta categoría se encuentran la Ingeniería Social, el *Trashing* y la Monitorización que se describen a continuación.

Ingeniería Social: Consiste en manipular a las personas para que ejecuten acciones indebidas en beneficio propio. Es una de las técnicas más efectivas para averiguar contraseñas de usuarios. Por ejemplo una persona se hace pasar por administrador del sistema solicitando a los usuarios a la comprobación de sus contraseñas.

***Trashing* o Cartoneo:** Consiste en revisar los papeles de un usuario determinado, ya que generalmente las personas anotan su *login* y *password* en algún papel (generalmente *post-it* adheridos al monitor) y cuando lo han aprendido lo botan a la basura. También, puede consistir en analizar buffers de impresora, memoria o bloques de discos buscando alguna información de la víctima.

Monitorización: Consiste en observar a la víctima y su sistema para obtener información. El escaneo de puertos, es otro método de monitorización ampliamente utilizado, su origen proviene de los sistemas de telefonía. Consiste básicamente, en enviar una serie de paquetes por diversos protocolos para poder obtener los servicios que están escuchando y que pueden ser vulnerables a un ataque. Los *Scanners* son herramientas esenciales de seguridad que permiten ahorrar numerosas horas de trabajo, pero estos, no son soluciones de seguridad integrales, sino que son un método que permite dar el primer paso en el tema de seguridad. El *packet sniffing* o *Eavesdropping* consiste en monitorear los paquetes que circulan por la red en un modo llamado promiscuo con el cual se pueden obtener paquetes destinados a otros equipos. La gran mayoría de los *sniffers* son detectables ya que están relacionados con el protocolo TCP/IP. El *snooping* al igual que el *sniffing* consiste en obtener información sin ser modificada, pero a diferencia del anterior se centra en el contenido de los paquetes. Esto es, documentos, mensajes, etc., y en la mayoría de los casos descargarla para hacer un análisis de la información obtenida.

2.3.3 Tipos de Ataques

Existen diferentes tipos de ataques, realizados principalmente por *Hackers*. En los principios de los 90, los ataques se realizaban con poca base técnica. Los *Insiders* (intrusos dentro de la empresa) utilizaban sus autorizaciones para alterar registros. Los *Outsiders* ingresaban solamente averiguando alguna contraseña valida. Al pasar los años, los ataques de se han diversificado y cada vez son más sofisticados y complejos. A continuación se muestran algunos tipos de ataques.

Ataques de Autenticación: El objetivo de este tipo de ataque es engañar al sistema para lograr ingresar a él. El *Spoofing* es un ejemplo de este tipo de ataques, que es precisamente actuar en nombre de otro usuario. Generalmente, el intruso utiliza un sistema para obtener información e ingresar a otro, y a otro. Esto, tiene como finalidad evitar la identificación del atacante y su ubicación real. Muchos de estos ataques comienzan con ingeniería social para obtener alguna contraseña de ingreso al sistema. El *Spoofing* es bastante conocido sobre todo el IP *Spoofing* y DNS *Spoofing*.

> ***Spoofing* de IP:** Técnica que permite al atacante tomar la identidad de un host "confiable" y obtener de este modo accesos no autorizados a otros sistemas.
>
> ***Spoofing* de DNS:** Técnica que permite al atacante poner en peligro un servidor de DNS y modificar de forma explícita las tablas de direcciones IP.

Las *Backdoors* y los *Exploits* también se encuentran en este grupo de ataques. Las *Backdoors* son trozos de código en un programa que permite saltarse los métodos de autenticación. Los *Exploits* permiten explotar agujeros de seguridad, ya sea por fallo o por error de sistema, lo que permite al intruso ingresar a él.

Denegación de Servicio (DoS): Un ataque de denegación de servicio (DoS) es una acción cuyo fin es incapacitar tanto hardware como software de un equipo, llevando a que no se pueda llegar al sistema y este deniegue el servicio. El objetivo principal es sacar a su equipo de la red. El DoS es un problema persistente ya que sus ataques son rápidos, fáciles y generan un resultado inmediato en la victima. Antes se veía como un juego se niños, pero ahora donde los servidores de las empresas cada vez toman mayor importancia (ej. Comercio Electrónico) un ataque de denegación de servicio podría provocar daños significativos para la empresa. Ejemplos de estos ataques son *Net Flood*,

Connection Flood y *Broadcast Storm* donde la idea principal es saturar la red con tráfico malicioso.

Ataques Web y de Modificación: Estos ataques se presentan generalmente debido a errores de diseño u operación de algún software. Dentro de esta categoría se encuentran los ataques mediante *Cross Site Scripting* (XSS), ActiveX, JavaScript, VBScript y Applets aprovechando la dejadez de parte de los usuarios de comprobar si estos elementos son seguros o no. El mal diseño de un software puede provocar un uso indiscriminado de éste si cae en las manos equivocadas como por ejemplo realizar ataques de *phishing*, obtener credenciales, modificar e infectar sitios web. Ejemplos de estos nuevos tipos de ataques son: *Cross-Context Request Forgery* (CCRF), *Cross-Context Scripting* (XCS) y *Command Fixation Attacks* (CFA) donde la idea principal es aprovecharse de las nuevas tecnologías para vulnerar sitios Web.

2.3.4 Virus

Los virus informáticos son programas que se copian automáticamente (programas que se replican y ejecutan por sí mismos) donde su principal objetivo es alterar el normal funcionamiento del equipo sin la autorización del usuario.[12]

Su origen se podría establecer al observar investigaciones de Inteligencia y Vida Artificial por John Von Newman en 1950 estableciendo la idea de programas auto replicables. En 1960, los laboratorios Bell desarrollaron juegos llamados *Core Wars* que competían por lograr el mayor espacio de memoria. Estos juegos, utilizaban técnicas de ataque, defensa, reproducción y ocultamiento que más adelante adaptaron los virus. En 1970, en el *Palo Alto Research Center* (PARC) de Xerox, John Shoch y Jon Hupp crearon programas auto replicables para controlar las redes informáticas. Pero, días después de su lanzamiento el programa se replicó a todas las maquinas y colapsó toda la red.

Los años 80 son sin duda el nacimiento de los virus informáticos como tal, y en 1983 se estableció una definición para ellos. En 1985 estaban infectando MS-DOS y en 1986 ya eran destructivos como por ejemplo *Brain*, *Vienna* y Viernes 13. El 2 de noviembre de 1988 se produjo el primer ataque masivo a una red y fue a ARPANET, el virus se replicaba por correo electrónico y en tres horas ya era conocido en todo EEUU. Su creador fue Robert Morris quien era hijo de uno de los programadores de *Core Wars*.

[12] Definición de Virus Informático http://es.wikipedia.org/wiki/Virus_informático

En 1991 aparecieron los primeros kits para la creación de virus. El precursor fue VCL *Virus Creation Laboratory* creado por alguien que se hace llamar Nowhere Man, lo que facilitó su crecimiento. En 1992 con la aparición del virus Michelangelo los virus alcanzaron mayor notoriedad y dejaron de ser curiosidad científica para convertirse en plaga. Principalmente, se aprovechan de las vulnerabilidades de los softwares, sistemas operativos, elementos de red, etc.

Los virus, habitualmente causan daños lógicos y en alguna ocasión daño físico. Para ello, sus creadores inventaron técnicas para poder ejecutar su programa. Algunas de ellas se presentan a continuación.

Archivos Ejecutables: El virus se adhiere a un ejecutable y desvía la atención del usuario ya que para él, el ejecutable realiza su ejecución de forma normal. El virus se aloja en la memoria e infecta otros programas que se ejecuten en la maquina. Estos, atacan principalmente a archivos con extensión .COM, .EXE, .DLL, etc. Por ejemplo, *Darth Vader*.

Virus del Sector de Arranque: En los primeros 512 bytes de un diskette se encuentra la función para arrancar o *bootear* un sistema desde el diskette, es esta área el objetivo de este tipo de virus. Al arrancar el sistema, el diskette ejecuta el virus el cual queda en memoria y luego ejecuta la zona de *booteo* original, lo cual parece normal para el usuario ya que nada extraño ha ocurrido ante sus ojos. Por ejemplo, Michelangelo, Diablo.

Macro virus: Son virus que afectan archivos de aplicaciones de oficina que tienen lenguaje de programación de macros. En el último tiempo, han tenido una gran expansión debido a que los usuarios realizan grandes intercambios de documentos. Los primeros virus de este tipo aparecieron para Lotus 1-2-3[13] pero su mayor difusión la tuvo con el procesador de texto Microsoft Word[14]. Estos virus, funcionan infectando la aplicación que los ejecuta, por ejemplo el procesador de texto y cada vez que este cree un nuevo o modifique algún archivo estará infectado. Ejemplos, en el caso de Word, CAP I y II.

[13] Lotus 1-2-3 http://www-01.ibm.com/software/lotus/products/123/
[14] Microsoft Word http://office.microsoft.com/word

Virus de Mail: Su modo de actuar es similar a los anteriores, pero se transmite vía email, cuando el usuario abre el mail y descarga el archivo este se ejecuta y se multiplica. Además, este tipo de virus se auto envía por las direcciones de correo en la libreta de direcciones, con lo que también saturan los servidores de correo. Ejemplos, Melissa, I Love You.

Caballos de Troya o Troyanos: Se basan en la mitología griega de la misma forma que el caballo de Troya. Los troyanos son programas aparentemente inofensivos que realizan una función útil, pero por debajo realizan una función desconocida para el usuario y que generalmente beneficia al autor del troyano y daña el sistema de la víctima. Si bien este tipo de programas no cumple con la condición de auto reproducción pero si cumple con ser un programa dañino.

2.4 Seguridad a Nivel de Red

El principal objetivo de las redes es mantener disponibles todos los equipos, datos y programas para cualquier usuario de la red, sin importar su ubicación geográfica. También, suministrar una alta fiabilidad, mediante distintos tipos de alternativas. El establecimiento de una red, puede proporcionar comunicación a personas que se encuentran alejadas geográficamente. La estructura física de la red la constituyen dos o más computadores que comparten recursos, pero una red es más que su estructura física ya que también la constituyen las personas que solicitan, proporcionan e intercambian información a través de los sistemas. Parece lógico, que los computadores se comuniquen entre sí cuando exista una conexión, pero que pasa si los equipos son de distintos fabricantes, distintos países. Para solucionar este tipo de conflicto es que nace un estándar para mejorar la comunicación entre los distintos equipos, este estándar es el modelo OSI que se definirá a continuación.

2.4.1 Modelo OSI

El modelo OSI (*Open System Interconnection*) es prácticamente utilizado en las redes de todo el mundo. Creado por el ISO (*International Standard Organization*), consiste en siete niveles o capas las cuales definen las funciones de los protocolos y cómo estos intercambian información para lograr comunicar varios sistemas. Cada nivel, depende del anterior que está debajo de él y le proporciona a los demás niveles superiores alguna funcionalidad específica. Estos niveles se definen a continuación.

Capa Física: Es la encargada de mantener el enlace físico entre los sistemas y del envío de bits por un medio físico de transmisión. Además, ofrece medios eléctricos y mecánicos para cumplir dicha labor.

Capa de Enlace: Es la encargada de tomar los bits entregados por la capa física y agruparlos en *frames*. Además, decide como acceder al medio físico y detecta anomalías o errores en los *frames* y se encarga de corregirlos.

Capa de Red: Es la encargada de controlar la operación de la red, como decidir la ruta para llevar los paquetes a su destino. Otra función es la resolución de cuellos de botella en la red.

Capa de Transporte: El objetivo de esta capa es tomar los datos de la capa de sesión y transformarlos para que puedan ser utilizados por la interfaz de red. Además, permite identificar y diferenciar múltiples conexiones mediante un mecanismo de nombres.

Capa de Sesión: Esta capa permite crear sesiones, sincronizar y establecer lugares de chequeo durante la conexión.

Capa de Presentación: Esta capa convierte los datos de las aplicaciones a un formato independiente de estas dándoles la facilidad para transmitir sus datos.

Capa de Aplicación: En esta capa están las aplicaciones de red que permiten explotar los recursos de otros sistemas.

Como se puede apreciar, todas las capas excepto la de aplicación, procesan los datos mediante operaciones para verificar que los datos estén íntegros y lleguen a su destino correctamente. En la Figura Nº4 que se muestra a continuación se puede apreciar más claramente el funcionamiento de este modelo.

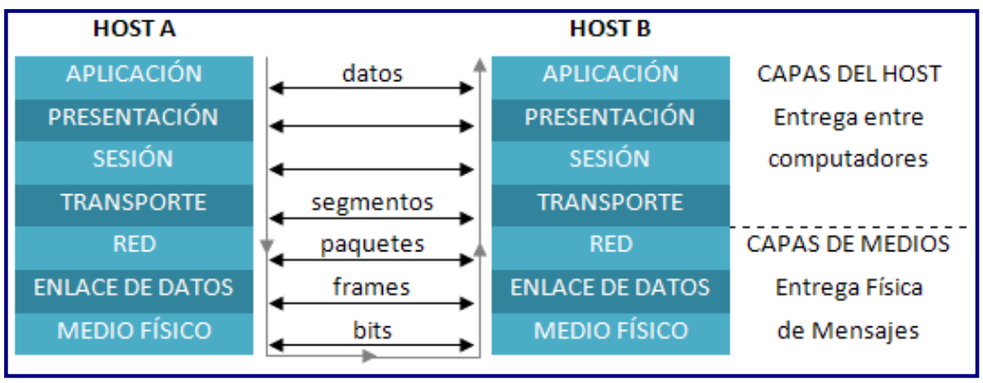


Figura Nº 4 Modelo OSI

En los años 80 apareció una red que se expandía por todo EEUU, lo que hoy es Internet pero para poder conectar los equipos a esta red, se establecieron reglas para lograr la comunicación e intercambio de información. Así, nacen los protocolos TCP/IP y posterior modelo TCP/IP que se detalla a continuación.

2.4.2 Modelo TCP/IP

Modelo de 4 capas principales basado en el modelo OSI y que se ha convertido en un estándar a nivel mundial. Esto, fue posible porque mientras se definía el modelo OSI los protocolos de TCP/IP ya estaban funcionando por ende estaba difundido por todo el mundo y pasó de la práctica a la teoría.

El TCP/IP (*Transmission Communication Protocol/Internet Protocol*) es hoy en día el protocolo más utilizado a nivel mundial por su independencia de Sistema Operativo y hardware. El TCP/IP no es un único protocolo, sino que son un conjunto de protocolos que cubren las cuatro capas de este modelo, donde los principales son los que le dan nombre al modelo el TCP y el IP. Las capas pertenecientes a este modelo se muestran a continuación.

Capa Interfaz de red: Corresponde al nivel físico y de enlace del modelo OSI. Los protocolos de este nivel se encargan de la transmisión a través del medio físico. Esta capa, funciona sobre algún tipo de red, que proporciona sus propios protocolos para el nivel de enlace, pero esto no es un problema ya que la función principal del TCP/IP es proporcionar abstracción del medio, lo cual permite el intercambio de información entre tecnologías diferentes aun cuando estas no sean compatibles.

Capa Internet: Equivale al nivel de red del modelo OSI, se encarga de enviar los paquetes a los destinos correspondientes, su protocolo principal es el IP.

Capa Transporte: Equivale al nivel de transporte del modelo OSI. Esta capa presenta dos grandes protocolos *Transmission Communication Protocol* (TCP) y *User Datagram Protocol* (UDP). Donde el primero, es orientado a conexión lo que significa que es un medio libre de errores para enviar paquetes o sea confiable. UDP en cambio, es un protocolo no orientado a conexión y no es confiable a diferencia del anterior. Esto se debe al distinto uso para el cual son empleados.

Capa Aplicación: Corresponde a los niveles de sesión, presentación y aplicación del modelo OSI. En esta capa están presentes los protocolos encargados de prestar servicios como por ejemplo HTTP y FTP.

El modelo TCP/IP está basado en el modelo OSI, pero este último no tuvo éxito debido principalmente a las demoras en la definición del mismo, la tecnología existente en ese momento y las malas políticas e implementaciones por parte de los investigadores. Pero es la combinación de ambos modelos la que permite las comunicaciones de hoy en día ya que OSI es un buen modelo y TCP/IP es un buen conjunto de protocolos. En la Figura Nº5, se muestra una comparación entre los dos modelos.

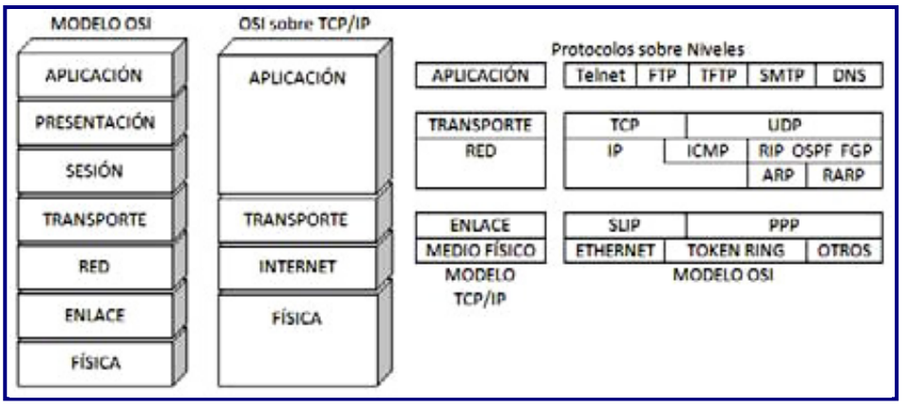


Figura Nº 5 Comparación Modelo OSI - TCP/IP

2.4.3 Elementos de Seguridad de Red

La seguridad de una empresa debe estar formada por múltiples componentes que permitirán ser un método mucho más efectivo para la disuasión de intrusos a los sistemas. Como por ejemplo, *Penetration Test*, *Firewalls*, Auditorias o *Logging*, Sistemas de detección de intrusos, etc. A continuación se definen algunos de estos elementos.

***Penetration Test*:** Es un conjunto de técnicas y metodologías que permiten realizar una estimación íntegra de las debilidades del sistema. Su objetivo es acceder a los sistemas y obtener privilegios de administrador, para poder realizar cualquier tarea en dichos sistemas.

***Firewalls*:** Es un equipo o programa que conecta dos redes (ej. una red local con Internet) impidiendo el acceso no autorizado según una política establecida. Estos sistemas, incorporan elementos que garantizan la privacidad, autentificación, etc. Con lo cual se impide el acceso no autorizado. Pero los *firewalls*, sólo sirven como defensa perimetral entre las redes, ya que no defienden de ataques dentro de la misma red, o de ataques que han burlado sus políticas de seguridad. Manejan el acceso a las redes y si estos no existieran todos los computadores de la red estarían expuestos a ataques desde el exterior. Además, el *firewall* es el punto ideal para monitorear la red, realizar *logs* y generar alarmas de ataque.

***Wrappers*:** Un *Wrapper*, es un programa que controla el acceso a un segundo programa y cubre la identidad de este segundo programa. El *Wrapper* más ampliamente utilizado es el TCP-*Wrappers*. El TCP-*Wrappers*, es un programa que es ejecutado cuando llega una petición a un puerto específico. Este, comprueba la dirección de origen y la verifica con reglas almacenadas y en función de ellas decide si dar el acceso o no. La utilización de *Wrappers* permite controlar el acceso a cada máquina y a los servicios accedidos, por ello, es un complemento ideal para un *firewall*.

***Intrusion Detection Systems* (IDS):** Es un componente más en el modelo de seguridad de una empresa. Su función principal es detectar acciones inapropiadas o anómalas en un sistema informático. La detección de intrusiones es la práctica de utilizar herramientas inteligentes y automáticas para detectar intentos de intrusión en tiempo real. Los IDS existentes se dividen en 2 grandes categorías:

> **Sistemas basados en normas:** Están basados en bibliotecas y bases de datos de ataques conocidos. Su desventaja principal es que dependen mucho del paso del tiempo ya que se debe tener actualizada la base de datos de ataques. Además, si un ataque es similar a otro pero no igual, afectará al sistema de igual forma, debido a que el IDS no lo conocerá como ataque.
>
> **Sistemas adaptables:** Emplean técnicas más avanzadas, tales como inteligencia artificial para ir aprendiendo y no sólo reconocer ataques. Su principal desventaja es su costo elevado, ya que son difíciles de mantener y se necesita conocimientos avanzados de matemáticas y estadísticas.

La idea principal de estos sistemas se basa en el hecho que una actividad intrusiva no actuará de manera normal con el sistema, a su vez el comportamiento del usuario tampoco será normal. Según el comportamiento las intrusiones se pueden clasificar como:

> **Falsos Negativos:** La actividad es una intrusión pero no es extraña para el sistema, y por ende no es detectada.
>
> **Falsos Positivos:** La actividad no es una intrusión, pero realiza un comportamiento extraño para el sistema, por lo cual el sistema “decide” que es intrusiva. Esto provoca poca confianza en los avisos generados por el sistema.

Negativos Verdaderos: La actividad no invasiva que el sistema detecta como tal.

Positivos Verdaderos: La actividad es invasiva y es detectada.

Las principales debilidades que presentan los IDS, radican principalmente en las falsas alarmas que generan y la actualización del comportamiento dependiendo del tipo de IDS.

***Logging*:** Es cualquier procedimiento por el cual un sistema operativo o aplicación graba eventos mientras estos ocurren y los guarda para un examen posterior. En el contexto de seguridad, el *logging* sirve con un propósito diferente, para tener un registro de las acciones dañinas de un atacante, ya que estos son la única evidencia real de lo ocurrido.

2.5 Intrusos y Delitos Informáticos

Los delitos informáticos son actividades criminales que se han tratado de enmarcar en los sistemas tradicionales, pero el uso de la Informática ha generado nuevos usos indebidos por lo que se ha hecho necesario legislar en cuanto a este tema. Existen distintos tipos de delitos informáticos. La Organización de Naciones Unidas[15] (ONU) reconoció los siguientes tipos de delitos[16]:

- Fraudes cometidos por manipulación de computadores.
- Manipulación de datos de entrada o sustracción de datos.
- Daños o modificaciones de datos o programas de computador.

2.5.1 Legislación Nacional

Chile fue el primer país latinoamericano en crear una Ley contra Delitos Informáticos. La ley 19223 publicada el 7 de junio de 1993 en el diario oficial, la cual señala que la destrucción o inutilización de un sistema informático puede ser castigado desde uno a cinco años de presidio. Esta ley no estipula condición de acceso al sistema, por lo que no sólo los intrusos pueden ser castigados sino que también, los creadores de virus.

El ingreso o *hacking* de un sistema, junto con el uso indebido de la información de este, también es susceptible a condenas de incluso cinco años de cárcel. Ahora, si se ingresa al mismo sistema, sin autorización y sin propósitos de ver el contenido no constituye delito.

[15] www.un.org/spanish
[16] http://www.delitosinformaticos.com/delitos/delitosinformaticos2.shtml

Por último, revelar la información de un sistema, es susceptible a condenas de hasta tres años de cárcel, pero si además es el responsable de dicho sistema la condena puede aumentar a cinco años.

En el Anexo A se puede apreciar mejor la ley 19223 y los cambios planteados desde 1993 a la fecha.

2.5.2 Tipos de Intrusos

Dependiendo de su forma de actuar, su nivel de conocimiento y los objetivos que persigue un intruso se puede clasificar en alguno de los tipos que se muestran a continuación.

***Hackers*:** Los *Hackers*, provienen de los tiempos de los técnicos de telefonía que arreglaban máquinas con un golpe, a estos técnicos se les llamaba *hackers* ya que la palabra *hack* significa golpear en ingles. A su vez, los *hackers* difieren mucho del estereotipo de joven ojeroso con lentes gruesos, ya que la mayoría son personas comunes y corrientes con cierto grado de curiosidad por la tecnología. Un *hacker*, no es *hacker* hasta que es reconocido por sus pares. Para obtener este reconocimiento y respeto de parte de sus pares un hacker debe realizar 5 acciones:

- Escribir programas útiles y donar los códigos fuentes a la comunidad.
- Ayudar, probar y depurar herramientas de software libre, como *beta-tester*.
- Filtrar y recoger información útil, tales como *FAQs* y ponerlos a disposición de la comunidad.
- Mantener el funcionamiento de la infraestructura de la comunidad, tales como foros de discusión, listas de correo, etc.
- Hacer algo por la cultura *hacker*. Donde siempre se recomienda la modestia.

Un *hacker* es una persona que vive para aprender, que le encantan los retos y lucha por la libre difusión de la información y la globalización de las comunicaciones. Un *hacker* no es un pirata ya que los piratas comercian la información que obtienen, mientras que los *hackers* obtienen la información sólo para uso personal.

Un mito en relación a los *hackers*, es decir que estos se dedican a destruir la información de los sistemas ajenos, esto es un error ya que los *Crackers* son los que destruyen la información de sistemas ajenos. En el peor de los casos, los hackers pueden ser perspicaces, maliciosos o curiosos exploradores.

***Crackers*:** Los *Crackers*, son personas cuyo objetivo va más allá de la simple investigación. Es una persona con fines malignos, haciendo daño solo por diversión o para demostrar sus habilidades. Según palabras de los propios *hackers*, estos consideran a los *crackers* como *hackers* mediocres, poco brillantes que buscan violar sistemas.

***Phreakers*:** El Phreakers viene de la fusión de palabras *Freak*, *Phone* y *Free*. Es la actividad en la que estos individuos engañan a las compañías telefónicas para realizar llamadas gratis. Los *Phreakers* son *Crackers* pero de las redes de comunicación, con amplios conocimientos en telefonía. Sus inicios se remontan a los sesentas cuando Mark Bernay descubrió un error de seguridad de parte de la empresa telefónica Bell. De ahí en más, aumento el número de personas que se aprovecharon de las deficiencias de dicha empresa, gracias a que la misma empresa se sentía tan orgullosa de su sistema que publicó detalladamente cómo era el funcionamiento de éste.

***Carding*:** El carding consiste en el uso ilegitimo de las tarjetas de crédito de otras personas para realizar fraudes. En un principio, los números y claves de tarjetas de crédito se podían obtener mediante un analizador de las señales electromagnéticas producida por los cajeros automáticos, con lo cual aumentó este tipo de personas.

Gurús: Los maestros y encargados de adiestrar a los futuros *hackers*. Se encargan de enseñar las técnicas básicas, aunque no están activos son reconocidos por la importancia de sus actos en el pasado.

***Lamers* o *Script Kiddies*:** Son los aficionados, que prueban todos los programas que llegan a sus manos. Se aprovechan de los conocimientos de otros para presumir. La mayoría de las veces son los responsables de lanzar virus o bombas lógicas por las redes.

***Wannaber*:** Son aquellas personas que desean ser *hackers* pero la comunidad considera que su coeficiente no está a la altura, pese a su actitud positiva es muy difícil que logre avanzar en sus planes.

Piratas Informáticos: Son aquellas personas que realizan copias ilegales de dispositivos audiovisuales o software tales como DVD, CD, etc. Para venderlos ilegalmente.

Samurái: Son la amenaza pura, saben lo que buscan, dónde y cómo encontrarlo. Trabajan a encargo y por dinero. No pertenecen a la comunidad. Se basan en que cualquiera puede ser atacado o saboteado, se podría decir que son una especie de asesino a sueldo moderno.

***Insiders*:** Individuos pertenecientes al personal de una organización que realizan ataques a los sistemas. Esto es muy alarmante ya que estas personas pueden conocer perfectamente los sistemas incluyendo los puntos débiles de este, pudiendo vulnerarlos más efectivamente que un atacante externo. Los tipos de *Insiders* pueden definir de acuerdo a la intención que puedan tener, algunos pueden ser:

- **Ex-Empleado:** Las personas pertenecientes a este grupo suelen estar interesados en violar la seguridad de la empresa, ya sea por haber sido despedidos o para sacar información para la competencia.
- **Curiosos:** Son los atacantes más habituales del sistema. En la mayoría de los casos son estudiantes con la intención de ingresar a los servidores o empleados que tratan de conseguir información prohibida para ellos.
- **Intrusos Remunerados:** Son los atacantes más peligrosos, ya que cuentan grandes conocimientos y experiencia, pero no son muy habituales. Generalmente son contratados por la competencia para robar información privilegiada, o simplemente arruinar la imagen de la empresa.

2.6 Resumen

En este capítulo se ha expuesto lo que significa el término de Seguridad Informática y como éste se aplica en distintos ámbitos como lo es la seguridad física, seguridad a nivel de software (lógica) o a nivel de red. Además, se vio el marco legal vigente en el país junto a aplicaciones que permiten asegurar sistemas informáticos. Por último, se presentaron los tipos de intrusos que afectan la seguridad de los sistemas informáticos, en que se diferencian y cuáles son sus formas de actuar.

De lo anterior se puede concluir que no existen los sistemas 100% seguros, así como no existe una herramienta exclusiva para el fortalecimiento de la seguridad de un sistema sino que un conjunto de herramientas que permiten hacer más complejo el acceso a los intrusos. Donde las políticas de la empresa juegan un papel fundamental dentro de la seguridad de sus sistemas.

Capítulo III HONEYPOT / HONEYNET

Antes de introducirse netamente en estas tecnologías, se debe recordar la historia que las precede, para conocer cómo estas nacieron y cómo lograron convertirse en lo que son.

Los primeros indicios de sistemas de monitorización de intrusos datan de 1990 en el libro “The Cuckoo’s Egg” de Clifford Stoll [STO90] y el trabajo de Bill Cheswick documentado en el libro “An Evening with Berferd” [CHE90]. A medida que pasaban los años se produjeron algunos hechos importantes como la realización en el año 1997 del Deception Toolkit por parte de Fred Cohen’s. En 1998 la creación de CyberCop Sting y NetFacade. Pero, sin lugar a dudas el hecho más importante ocurrió en abril de 1999 [KUE01], cuando un grupo de expertos en Seguridad Informática mediante correos cruzados de la lista de correo “Wargames” lograron el desarrollo formal del proyecto Honeynet Project.

En la Tabla Nº2 que se muestra a continuación se pueden apreciar los principales hechos relacionados con la historia de los Honeypots.

Tabla Nº 2 Hechos principales en la Historia de los Honeypots

Año	Hecho Importante
1990	- Honeypot conceptos publicados por Clifford Stoll en “The Cuckoo’s Egg” - Bill Cheswick "An Evening with Berferd"
1997	Fred Cohen’s realiza el Deception Toolkit
1998	- CyberCop Sting - honeypot comercial - BackOfficer Friendly es realizado - Marty Roesch y GTE Internetworking trabajan en NetFacade. Esto es el comienzo del concepto de Snort
1999	Nace The Honeynet Project
2000	Honeypots usados para capturar y estudiar gusanos
2002	- Un honeypot fue usado para detectar y capturar un ataque desconocido, el Solaris dtspcd exploit. - The Honeynet Research Alliance
2004	Concepto de colección de malware
2005	Unknown worm (Dasher) fue capturado por Honeynet Research Alliance

En Junio de 2000, el honeypot del Honeynet Project fue atacado y comprometido por un famoso grupo de hackers, lo cual permitió estudiar su comportamiento “online” y demostrar la utilidad y viabilidad de esta nueva herramienta de seguridad.

Ya en el año 2001 Honeynet Project se convierte en una organización sin fines de lucro dedicada al estudio de la comunidad blackhat. En el año 2002 se crea la The Honeynet Research Alliance [THE08], que es un foro de confianza de organizaciones de investigación. Las organizaciones miembros de la Honeynet Research Alliance no son parte del Proyecto Honeynet. En lugar de ello, son entidades independientes.

Estas organizaciones se suscriben a la Alianza con el propósito de investigación, desarrollo y despliegue de las tecnologías relacionadas con los Honeypots y compartir las lecciones aprendidas.

Pero sin lugar a dudas el hecho más importante relacionado con este tipo de tecnologías, es el libro "The Art of War" de Sun Tzu. Sun Tzu, quien fue un general militar chino, un mercenario y aristócrata que vivió en los años 544-496 AC. En su libro destaca la necesidad de conocer el comportamiento del enemigo antes de enfrentarse a éste en una batalla. Ya que al conocerlo, se podrá saber el resultado de ésta.

3.1 Honeypot

Para definir Honeypot se utilizará la definición realizada por Lance Spitzner [SPI02] como:

> “Un recurso de seguridad destinado a ser atacado o comprometido por atacantes. Su finalidad no es en ningún caso, resolver o arreglar fallas de seguridad. Sino que se encarga de proporcionar información valiosa sobre posibles atacantes en la red antes de que comprometan sistemas reales”

El concepto de honeypot no fue algo que salió de la nada, sino que es el fruto de la investigación desarrollada en el campo de la Seguridad Informática [SCH99].

Los Honeypots en su forma más básica son servidores falsos, ubicados estratégicamente, los cuales son nutridos con información falsa que es encubierta como archivos confidenciales. Estos servidores son configurados de forma que sea difícil más no imposible ser comprometidos por un atacante, exhibiéndolos intencionalmente y haciéndolos altamente llamativos para un “hacker” en busca de un blanco.

Por último, el servidor es preparado con herramientas de monitoreo y rastreo de información, de manera que cada hecho y rastro de actividad de un “hacker” sea registrado en una bitácora de manera detallada.

Las funciones principales de un Honeypot son [HER]:

- Desviar la atención del atacante de la red real del sistema, de manera que no se comprometan los recursos principales de información.
- Capturar nuevos virus o gusanos para su estudio posterior.
- Formar perfiles de atacantes y sus métodos de ataque preferidos, de manera similar a la usada por una corporación policiaca para construir el archivo de un criminal basado en su modus operandi.
- Conocer nuevas vulnerabilidades y riesgos de los distintos sistemas operativos, entornos y programas las cuales aún no se encuentren debidamente documentadas.

3.1.1 Ventajas

Un Honeypot tiene un significado relativamente sencillo, y entrega una fortaleza muy sólida. Podemos observar sus ventajas en los siguientes puntos:

Nuevas Herramientas y Tácticas: Son diseñados para capturar cualquier interacción con estos, incluso herramientas o tácticas nunca antes vistas o 'zero-days'.

Recursos Mínimos: Esto significa que los recursos pueden ser mínimos y aún así se puede implementar una plataforma lo suficientemente poderosa para funcionar en gran escala.

Encriptación en IPv6: A diferencia de las tecnologías de seguridad más comunes, los Honeypot también se pueden utilizar en ambientes sobre IPv6, detectando un ataque sobre IPv6 de igual forma que lo hace con un ataque sobre IPv4.

Información: Recopilan información de forma detallada a diferencia de otras herramientas de análisis de seguridad, reduciendo los falsos negativos y falsos positivos.

Simplicidad: Gracias a su arquitectura, son conceptualmente simples. Mientras más simple es la tecnología, menos posibilidades de errores habrán.

3.1.2 Desventajas

Los Honeypots tienen debilidades propias a su diseño y funcionamiento como cualquier otra tecnología. Esto se debe a que utilizan las tecnologías existentes y no reemplazan a las tecnologías actuales, estas debilidades son presentadas a continuación:

Visión Limitada: Sólo permite registrar y capturar actividad con la cual interactúa directamente. No capturan información de ataques destinados a otros sistemas, a menos que el agresor o la amenaza interactúen con el Honeypot al mismo tiempo.

Riesgo: El uso de cualquier tecnología de seguridad implica siempre un riesgo potencial. Los Honeypots no difieren a esto ya que también corren riesgos, específicamente el de ser secuestrados e intervenidos por el atacante y ser utilizados como plataforma de lanzamiento de otros ataques.

3.1.3 Clasificación

Los Honeypots se pueden clasificar de acuerdo a dos razonamientos: Según su Ambiente de Implementación y según su Nivel de Interacción. Estos razonamientos de clasificación hacen más fácil comprender su operación y utilización al momento de idear la implementación dentro de una red o infraestructura de TIs.

3.1.3.1 Honeypot según su ambiente de Implementación

En esta clasificación se especifican dos tipos de Honeypots: De Producción y de Investigación.

Honeypots de Producción: Se utilizan para resguardar a las organizaciones en situaciones reales. Se implementan de forma adyacente a las TIs y están sujetas a ataques constantes las 24 horas del día, 7 días a la semana. Se les atribuye cada vez más importancia por las herramientas de detección que brindan y por la forma cómo pueden complementar la protección de la red. Su valor reside en la Protección, Detección y Respuesta. Ejemplos: BackOfficer Friendly, LaBrea Tarpit, Deception Toolkit, Smoke Detector, Specter, Honeyd.

Honeypots de Investigación: Estos Honeypots no son implementados con la finalidad de proteger redes, sino que constituyen recursos educativos de naturaleza demostrativa y de investigación cuyo objetivo se centra en estudiar patrones de ataque y amenazas de todo tipo junto con dar alertas tempranas y predecir los ataques. Se utilizan para recolectar información sobre las acciones de los intrusos. El proyecto Honeynet, por ejemplo, es una organización de seguridad voluntaria, sin fines de lucro que utiliza Honeypots para recoger información de las amenazas que ocurren en el ciberespacio. Su valor reside en la Predicción y Alerta Temprana. Ejemplos: ManTrap, Honeynet.

3.1.3.2 Honeypots según su Nivel de Interacción

Los objetivos de los Honeypots son distintos. Cuanto más logre hacer un intruso en un Honeypot, más alto es el nivel de interacción. Cuanto mayor nivel interacción más se puede conocer sobre el intruso y aumenta el riesgo. Los Honeypot de producción suelen tener baja interacción mientras que los de investigación alta interacción.

“Nivel de interacción” es un término creado para comprender las capacidades de los distintos Honeypots. Es lo que se emplea para medir cuánta funcionalidad ofrece un Honeypot a su atacante. Cuando un atacante interactúa con un Honeypot hay distintos niveles de funcionalidad que éste puede ofrecer. Algunos Honeypot ofrecen sólo un conjunto limitado de servicios emulados, mientras que otros incluso sistema operativos reales al que puede conseguir acceder el atacante. Si lo único que un atacante puede realizar es conectarse a un Honeypot, sólo se capturarán las conexiones realizadas. Sin embargo, si el atacante dispone de un sistema operativo real al cual conectarse y con el cual interactuar, se podrá aprender más de él.

El nivel de interacción que se quiera depende de lo que se quiere conseguir. Además, en función del nivel de interacción que se escoja las ventajas y desventajas cambiaran. Esto, es un asunto de suma importancia en el momento de escoger que Honeypot se necesita y como implementarlo.

Estas categorías ayudan a comprender no sólo el tipo de Honeypot con el cual se trabaja, sino que también a definir el rango de opciones de vulnerabilidades que se desea que un atacante explote. Estas son las características de mayor relevancia al momento de construir el perfil de un atacante.

Honeypots de Baja Interacción: Los Honeypots de baja interacción generalmente ofrecen servicios emulados. La interacción del intruso estará limitada por la funcionalidad que ofrezcan estos servicios. Los Honeypots de baja interacción se utilizan comúnmente como Honeypot de producción para proteger redes, ya que capturan poca información como para poder ser utilizados como un sistema de investigación. Se utilizan generalmente como tecnologías de engaño o detección. La mayor parte de los Honeypots tradicionales son de baja interacción.

La principal ventaja de este tipo de Honeypot es su simpleza, ya que es fácil de manipular y mantener, siempre manteniendo un riesgo menor. Por ejemplo, un servicio FTP emulado, escuchando en el puerto 21, probablemente estará emulando un login FTP o probablemente soportará algunos comandos FTP adicionales, pero no representa un blanco crítico ya que probablemente no está relacionado a un servidor FTP que contenga información sensible.

Su principal desventaja es que sólo registran información limitada, ya que sólo están preparados para capturar actividad predeterminada. Esto se debe, a que los servicios emulados sólo llegan hasta un cierto límite operacional, ésa característica limita el rango de opciones que se pueden mostrar al potencial intruso. De igual forma, para un atacante con ciertos conocimientos es relativamente simple detectar este tipo de Honeypot. Ejemplos: KFSensor, BackOfficer Friendly, Specter y Honeyd.

Honeypots de Media Interacción: Permite algo de interacción con el sistema operativo, pero con funcionalidades limitadas. El mejor ejemplo de esto, es trabajar en el entorno chroot del sistema operativo.

Honeypots de Alta Interacción: Los Honeypots de alta interacción no emulan nada. En lugar de esto se les da a los atacantes un sistema operativo real completo con el que pueden interactuar. Los atacantes pueden descargar ficheros, binarios de troyanos, compilar código o múltiples otras acciones. Debido a esto, se puede capturar gran cantidad de información. La información que se almacena no solo incluye las técnicas de sondeo y de explotación empleadas sino que también permitirá al administrador de seguridad observar al atacante una que vez que este obtenga acceso al sistema y exponga de manera inconsciente sus intenciones y herramientas. Utilizados principalmente para investigación y respuesta, pero también pueden ser utilizados para prevención y detección.

Este tipo de Honeypot, no sólo puede ser utilizado como elemento de engaño y detección, sino que también puede ser utilizado para responder ante incidentes y para investigar a los atacantes. Se pueden capturar pulsaciones, nuevas herramientas de ataque, imágenes e incluso conversaciones.

Las principales ventajas son dos: La capacidad de capturar gran cantidad de información vinculada al modus operandi de los atacantes. De esta forma, se pueden comprender todas sus acciones, tales como nuevos rootkits, zero-days y sesiones de IRC. La segunda ventaja, es que los Honeypots de Alta Interacción no asumen un posible comportamiento que podría tener un atacante, proporcionando entonces, un ambiente abierto para capturar todas las actividades realizadas por éste. Esto, permite a este tipo de Honeypot conocer comportamientos inesperados.

Sin embargo, esta última capacidad incrementa el riesgo de que los atacantes puedan utilizar estos Honeypots para atacar a otros sistemas, convirtiéndolos en un arma para el intruso. En consecuencia, se requiere la implementación de una tecnología adicional para prevenir que el atacante dañe otros sistemas o que limite al sistema comprometido a que no pueda convertirse en una plataforma para el lanzamiento de ataques. Hoy por hoy, el mejor ejemplo de un Honeypot de alta interacción está representado en las Honeynets y en ManTrap.

En la Tabla Nº3 se puede apreciar un resumen de los 2 niveles más importantes de interacción.

Tabla Nº 3 Diferencias en los principales tipos de Honeypots

Baja Interacción	Alta Interacción
Emulación de servicios	Servicios, Sistemas Operativos y aplicaciones reales
Bajo Riesgo	Alto Riesgo
Fácil de desarrollar y mantener	Difícil de desarrollar y mantener
Captura información cuantitativa de los ataques	Captura una extensa cantidad de información valiosa.
Ej.: Honeyd, nepenthes, labrea,…	Ej.: Gen II Honeynets

Cuando los Honeypots se utilizan con fines productivos, entregan protección mediante prevención, detección y respuesta a un ataque. Cuando son utilizados con fines investigativos, recolectan información que depende del contexto bajo el cual hayan sido implementados. Algunas organizaciones prefieren estudiar las tendencias que siguen las intrusiones, otras en cambio, prefieren la prevención y predicción anticipada a los ataques.

Ninguno de los niveles de interacción es mejor que otro, cada uno tiene sus ventajas y desventajas, todo depende de lo que se quiera conseguir con la implementación del Honeypot, seleccionando el nivel de interacción dependiendo del objetivo que se quiera alcanzar.

3.1.4 Aspectos Legales

El uso de Honeypots implica tener alcances legales según el tipo de uso que se les dé. Por ejemplo, la ley norteamericana protege la inviolabilidad de las comunicaciones personales (interception of communications) de forma muy estricta. El punto es que dependiendo del tipo de Honeypot que se utilice, se puede violar dicha ley al recoger una cantidad de información sobre el atacante que la ley protege explícitamente [POU03].

El espiar al atacante teniendo comunicación desde la red hacia terceros es el problema fundamental, ya que el atacante podría demandarnos por invasión a la privacidad. Por ello es fundamental dejar en claro cuáles serán los objetivos del Honeypot para así no estar fuera de la ley.

Según Lance Spitzner [SPI03] existen 3 temas principales de responsabilidad legal derivados del uso de Honeypots:

Privacidad (*Privacy*): La información capturada por un Honeypot se puede dividir en dos tipos, información transaccional e información de contenido.

La información transaccional es aquella que se obtiene netamente de aspectos técnicos como la dirección IP del atacante, la fecha, los paquetes, etc.

La información de contenido en cambio, es la información de la comunicación del atacante con terceros. Este es el punto de conflictos legales, según los autores de libros relacionados con el tema, se debería incluir un mensaje de advertencia que permita excusarse a esto. En la Figura Nº6 se presenta un ejemplo de este tipo de mensaje.

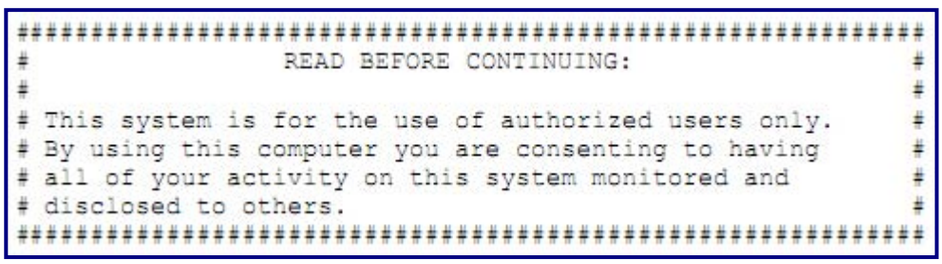


Figura Nº 6 Ejemplo de mensaje de advertencia

Trampa (*Entrapment*): Proceso realizado por la policía para inducir a una persona a realizar una acción ilícita con el fin de iniciar una demanda judicial contra él. Cómo el Honeypot es construido para ser comprometido, el fin de éste no es perseguir al atacante mediante una demanda judicial, sino que recibir sólo los ataques para su estudio posterior.

Responsabilidad (*Liability*): Esto toma en cuenta las posibles demandas judiciales que se pueden recibir en el caso de que un atacante utilizará el Honeypot como plataforma de lanzamiento de ataques. Estas demandas se basarían en que la red constaba con las mínimas medidas de seguridad e incluso facilitaba el acceso a los atacantes.

Cualquier organización puede ser responsable si su red se utiliza para atacar o dañar a terceros aunque esta no contenga Honeypots. Por este motivo el Proyecto Honeynet presta tanta atención al Control de Datos.

3.2 Honeynet

Una Honeynet NO es una red de Honeypots. Una Honeynet es: “un tipo de Honeypot, que define una arquitectura de red con las mismas intenciones que un Honeypot donde no se emula nada. Se trabaja con SSOO reales y Servidores/Aplicaciones reales, es altamente interactivo, diseñado para la investigación y la obtención de información sobre atacantes”. Cualquier tráfico que entre o salga de la Honeynet es sospechoso por naturaleza [THE03b].

Su objetivo es estudiar las técnicas y motivos de la comunidad blackhat y responder a las 5+1 W’s de los incidentes de seguridad: *What, where, when, who, why* + *How*. La Honeynet, en lugar de suministrar un destino donde los paquetes vayan a morir, permite que ocurra la conexión (*handshake*) y se establezca un diálogo bidireccional completo. El objetivo que persiguen los distintos tipos de Honeypots es el mismo para todos y es aprender las tácticas del atacante y obtener la mayor cantidad de información posible sobre este.

Las ventajas de la Honeynet son que cualquier trafico que pasa por ella es ilegítimo por naturaleza por lo mismo permite reducir el número de falsos positivos. Además, permite detectar nuevos tipos de ataques conocidos como zero-days y entregar una notificación temprana de los incidentes.

3.2.1 Características

Una Honeynet presenta 3 requerimientos básicos para ser realmente útil y que permita la extracción de información valiosa tal como lo muestra la figura siguiente.

Control del flujo de datos (Data control): Éste, especifica las decisiones sobre el filtrado o enrutado de los paquetes y restringe el acceso de la Honeynet a la red de producción. Mantiene un control constante del flujo de datos para evitar que el atacante la utilice contra terceros o contra nuestra propia red.

Si bien es cierto que cuanta más interacción se permita con el exterior más datos reales se podrán obtener, por este motivo se debe evaluar los riesgos que conlleva. Si sólo interesa el ataque, se puede denegar todas las conexiones salientes, pero si se quiere ver qué intenta hacer después, se necesita darle mayor libertad. En la Figura Nº7 que se muestra a continuación se puede ver más claramente como ocurre el control de los datos.

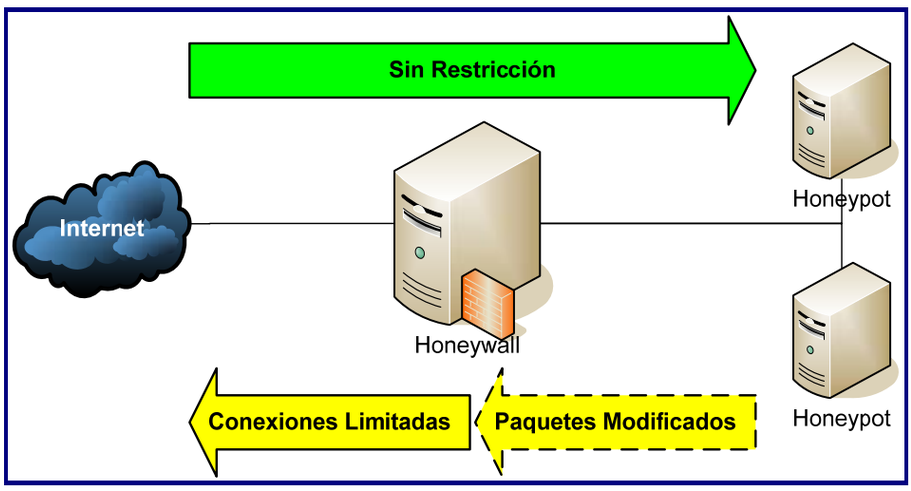


Figura Nº 7 Funcionamiento del control de datos

Captura de datos (Data capture): La captura de todos los movimientos y acciones que realice el atacante en la Honeynet revelará sus técnicas y motivaciones por ende el poco tráfico que se captura tiene un grandísimo valor. Si bien es primordial que el nivel de vigilancia y captura sea alto, si este es excesivo o descubierto por el atacante dejará de ser efectivo.

La captura de datos se debe hacer con bastante sigilo y sin despertar ningún tipo de sospecha, por lo que debe ser planificada cuidadosamente. El lugar para almacenar la información debería hallarse fuera de la Honeynet, ya que si un sistema es comprometido, dicha información puede ser encontrada o incluso peor, falseada o borrada. Además, si se quiere capturar los registros, éstos suelen enviarse a un servidor inexistente para que los capture la máquina que está en modo promiscuo.

Algunos métodos para la captura de datos son: Logs del firewall (iptables), Alertas del IDS (Snort), Identificación pasiva de SO (p0f), Captura avanzada de datos (Sebek), Tráfico de red (tcpdump) y Alertas del IPS (Snort-inline). En la Figura Nº8 se muestra como Sebek permite realizar una captura avanzada de los datos.

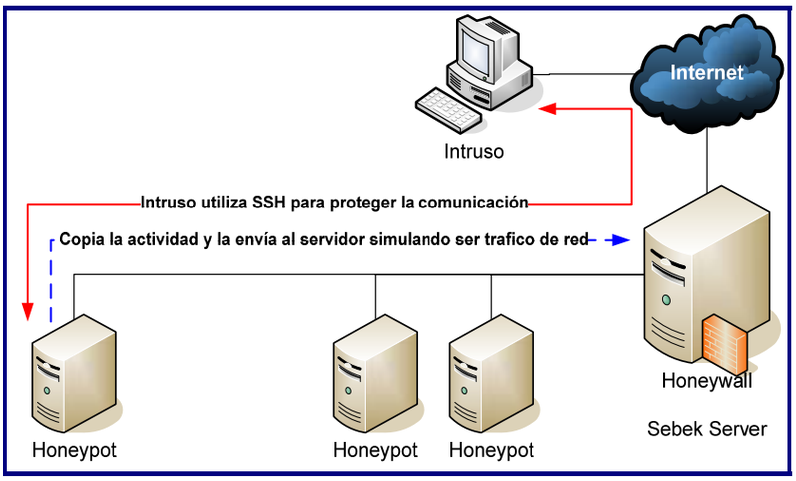


Figura Nº 8 Captura avanzada de datos con Sebek

Sebek actúa complementandose al kernel del Sistema Operativo lo que hace más dificil su detección permitiendo capturar los datos del atacante sin que éste se de cuenta que es observado.

Análisis de Datos (Data Analysis): Realiza análisis de la información obtenida del atacante permitiendo correlacionar los datos obtenidos. Además, permite graficar la información obtenida haciendo más intuitivo el análisis de los datos. De otro modo, permite realizar ingeniería inversa y recolección de los datos cuando el o los equipos han sido comprometidos también llamado análisis forense.

En la Figura Nº9 se muestran estos tres elementos básicos y las herramientas que permiten contar con estos elementos en una Honeynet.

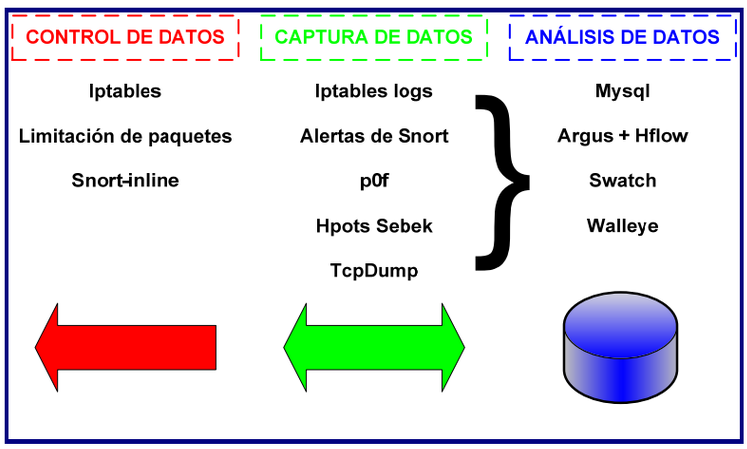


Figura Nº 9 Herramientas utilizadas en las Honeynet

La mayoría de los sistemas de seguridad han sido siempre de carácter defensivo como por ejemplo IDS y Firewalls. Éstos, intentan defender los sistemas de ataques. Por ende, si no se recibe ningún tipo de ataque, los sistemas permanecerán sin mejorar o mejor dicho sin la pro-actividad que necesitan tener los sistemas de seguridad.

Las Honeynets intentan realizar un cambio frente a esta actitud, mediante el estudio de los ataques y atacantes. Sin Honeynets, cada vez que se origine un nuevo ataque a un sistema de la organización, éste dejará de dar servicio y pasará a estar comprometido. En cambio con las Honeynets, un ataque exitoso no debería afectar a ningún sistema real.

Existen muchas ventajas con la instalación de una Honeynet dentro de una organización, tales como desviar la atención de los atacantes de los servidores principales de la organización. Detectar ataques tanto externos como internos junto con detectar ataques automatizados. Maneja un menor volumen de datos que las herramientas tradicionales de seguridad. Sin embargo, los datos obtenidos son de altísimo valor.

A medida que pasa el tiempo la instalación y configuración de una Honeynet se hace cada vez más simple. Esto se debe a las personas que trabajan en el proyecto Honeynet, que en su investigación del tema han realizado un CD que basado en una distribución de Linux permite la instalación de una herramienta llamada Honeywall, la cual permite realizar la captura, control y análisis de los datos obtenidos de la Honeynet. Además, han desarrollado scripts de configuración y paquetes de instalación de herramientas anexas.

3.2.2 Proyecto Honeynet

El Proyecto Honeynet es una organización voluntaria sin fines de lucro formada por profesionales de la seguridad dedicados a investigar amenazas cibernéticas y compartir las lecciones aprendidas. Sus principales objetivos son incrementar el conocimiento e informar sobre las amenazas existentes.

El Proyecto nació de una lista de correos llamada Wargames en abril de 1999 y en junio de 2000 se convirtió en el Proyecto Honeynet. Cuenta con una junta directiva de no más de dos miembros de la misma organización. En el año 2002 nace un foro de las organizaciones pertenecientes al proyecto llamado The Honeynet Research Alliance que comparte y despliega tecnologías relacionadas con las Honeynet.

3.2.3 Arquitecturas

Hasta el momento existen 3 tipos de arquitecturas que se diferencian por las funcionalidades que poseen y los electos básicos que presentan.

3.2.3.1 Gen I

La primera generación implementa sólo elementos de control del flujo de datos y captura de datos. Son los primeros Honeypots de alta interacción y vieron la luz en 1999. Además, su arquitectura de red consta de tres subredes separadas por un firewall, donde las subredes son Internet, la red reproducción y la Honeynet. En la Figura Nº10 se puede apreciar más claramente la arquitectura de red de esta generación.

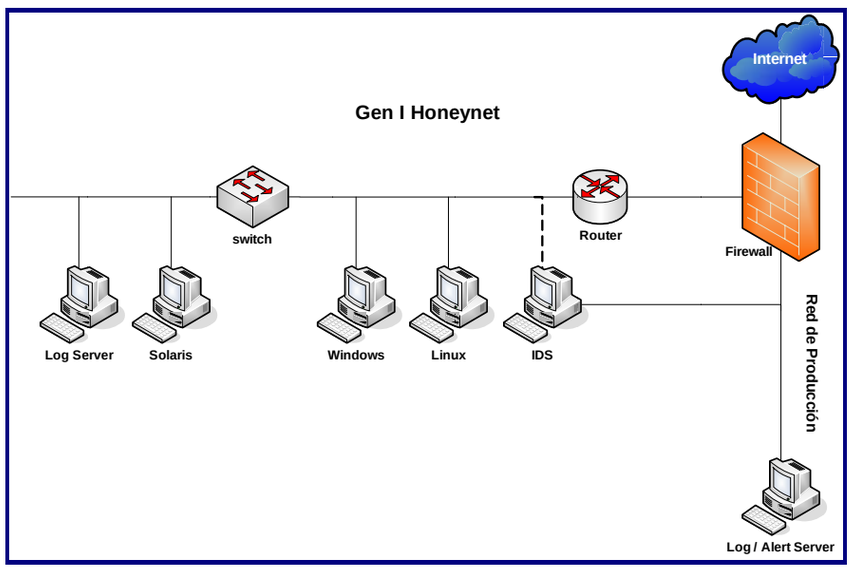


Figura Nº 10 Arquitectura de red Gen I

El control de las redes es realizado por el firewall. El *router* es utilizado también como medio de control y filtrado de paquetes. El firewall sólo permite un cierto número de conexiones, este número dependerá de cuán atractiva para el atacante se quiere la Honeynet. En la Figura Nº11 se muestra un ejemplo del control de datos utilizado.

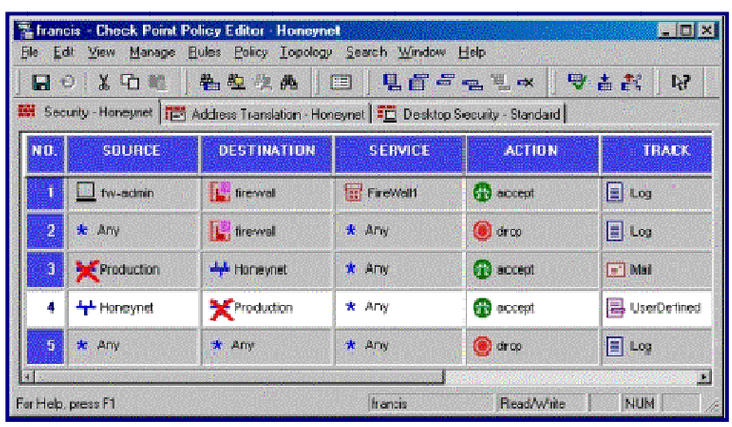


Figura Nº 11 Ejemplo de control de datos Gen I

El control de datos se realiza de dos formas, bloqueando conexiones o limitando el número de conexiones. Una característica de esta generación es que opera a nivel de capa 3 (IP) por ende puede ser accedida remotamente. Es buena atrapando a intrusos fáciles como Script Kiddies pero si los atacantes tienen mayor conocimiento estos la detectaran fácilmente.

La captura de datos se inicia en el firewall, ya que recibe todos los paquetes de entrada y salida. La captura del tráfico en la Honeynet es realizada por el IDS. Esta se divide en cuatro categorías que son captura de las transacciones de la red, captura del tráfico de la red, captura de las actividades del Host y las alertas del IDS. Para asegurar que el atacante no encuentre la información obtenida, ésta es enviada diariamente a un computador “seguro” para luego ser analizada.

La Gen I se puede detectar fácilmente porque una vez se ha entrado al sistema, sólo se puede acceder al resto de servidores y a una máquina sin servicios que justamente está en modo promiscuo.

3.2.3.2 Gen II

Las Honeynets de segunda generación nacidas en el año 2002 se caracterizan porque combinan los elementos de la primera generación en un solo dispositivo llamado Honeywall. Por lo tanto, el control de flujo de datos, la captura de datos y la recolección de datos están concentrados en un solo dispositivo.

Este Honeywall es un dispositivo de capa 2 (Gateway) que permite transmitir los paquetes en tipo puente (bridge). Esta capacidad, permite al Honeywall parecer invisible dentro de la red, ya que se encarga de enviar por un extremo lo mismo que recibe por el otro.

Esta unión de funcionalidades en un único dispositivo facilita la instalación y administración de la Honeynet. Además, por su actuación como dispositivo transparente hace mucho más difícil su detección por parte del atacante. En la Figura Nº12, se presenta un ejemplo de arquitectura típica de la Gen II.

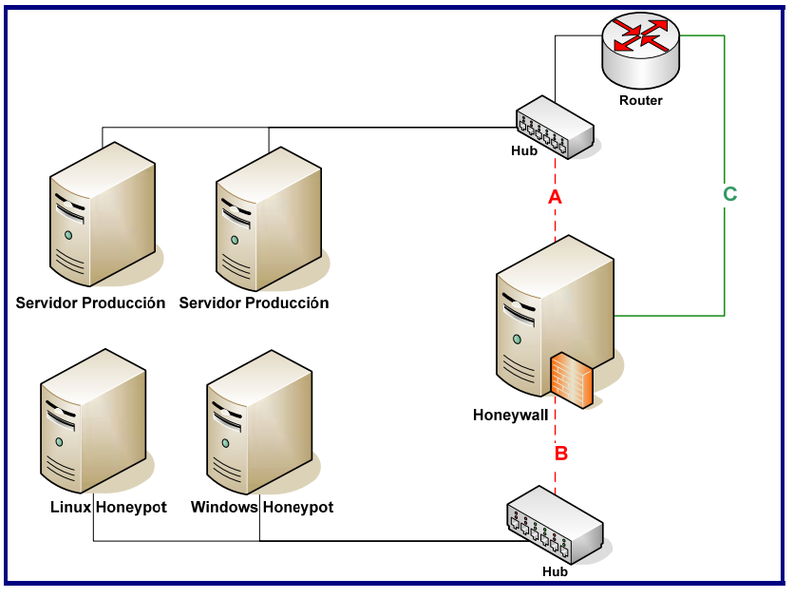


Figura Nº 12 Arquitectura típica de una Honeynet GEN II

En el esquema pareciera que existieran dos redes, la de producción y la Honeynet pero sólo es una. Como el Honeywall funciona en capa 2, es como si el equipo no existiera ya que no tiene dirección IP. Esto es porque las interfaces A y B funcionan a nivel de capa 2 en modo *bridge*. La interface C si tiene una dirección IP y permite administrar y controlar el Honeywall.

La Gen II muestra mejoras en relación a la Gen I, la primera es a nivel del control del flujo de datos, ya que en la Gen II se tiene un control total de las conexiones no importando si tiene un límite establecido como en la Gen I.

La segunda mejora radica en la forma de responder las actividades no autorizadas ya que no bloquea los accesos, sino que los puede modificar en tiempo real los datos lo que dificulta la detección por parte del atacante. Esto le añade a las funciones de bloqueo cierta capacidad de un sistema de prevención de intrusión en la red o NIPS.

La herramienta Sebek2 incorporada en el Honeywall permite capturar la información aun cuando se utilice un medio cifrado ya que funciona a nivel de kernel del Sistema Operativo. Además, cuenta con programas que permiten limitar la cantidad de conexiones por unidad de tiempo, junto con monitorear y cambiar las reglas del firewall. También se puede limitar el ancho de banda utilizado pero esta opción no es muy común.

3.2.3.3 Gen III

Las Honeynets de tercera generación nacidas en el año 2003 se caracterizan por integrar análisis de datos en el mismo dispositivo Honeywall, lo que hace más sencillo su utilización y mantención. Aunque no fue hasta mayo de 2005 con la aparición del Honeywall Roo que pasó a suceder a la generación anterior.

La Gen II y III se caracterizan por tener la misma arquitectura. Pero se diferencian por las mejoras que tiene la Gen III en cuanto la gestión y el desarrollo.

El Honeywall de la Gen III cuenta con herramientas como Hflowd, pcap_api y Walleye que permite correlacionar los datos obtenidos. Walleye es una interfaz Web que permite administrar el sistema y provee de interfaces a Hflowd y pcap_api para realizar el análisis de los datos. En la Figura Nº13 se puede observar un ejemplo de una arquitectura típica de la Gen III.

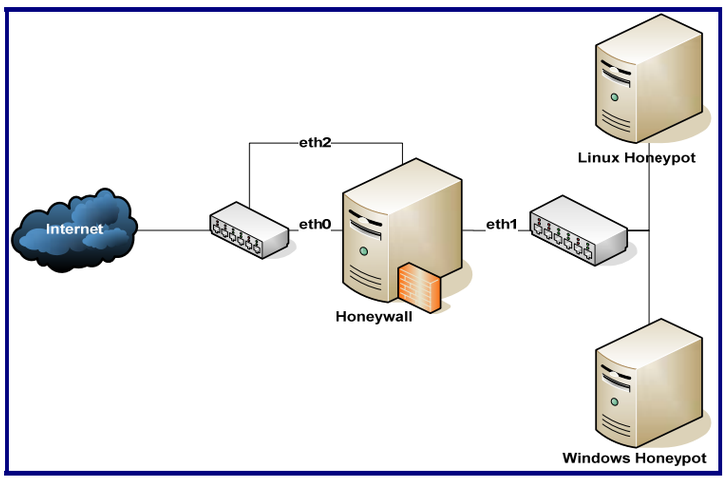


Figura Nº 13 Arquitectura típica de una Honeynet GEN III

En la Tabla Nº4 se puede observar una comparativa que permite apreciar las diferencias reflejadas entre estas tres generaciones de Honeynet.

Tabla Nº 4 Tabla Comparativa de las distintas Generaciones

	Gen I	Gen II	Gen III
Control de Datos	Si	Si	Si
Captura de Datos	Si	Si	Si
Análisis de Datos	No	No	Si
Nivel de Operación	Capa de Red	Capa de Enlace	Capa Enlace
Detectable	Fácilmente	Difícilmente	Difícilmente
Información Cifrada	No Captura	Si Captura	Si Captura
Interfaz Web	No	No	Si
Informes Automatizados	No	No	Si

3.3 Wireless Honeypots

Las redes Wireless han ido en aumento con el pasar de los años. Pero como cualquier otra red no está exenta de accesos no autorizados o ataques perpetrados por hackers. Sin embargo en este tipo de redes es más crítico debido a tres factores fundamentales:

- Las especificaciones y estándares en estas redes son relativamente nuevos por lo cual pueden permitir algún fallo o error. Es ahí donde apuntan los atacantes para obtener acceso a este tipo de redes.

- La facilidad de conexión que presentan la redes inalámbricas permite a cualquier dispositivo acceder de manera fraudulenta a la red, ya que estos no necesitan estar conectados físicamente, lo que provoca que el ataque pueda ser realizado desde cualquier sitio.

- La movilidad que proporciona este tipo de redes permite a los atacantes ir cambiando su ubicación haciendo más difícil detectar el lugar del ataque.

La utilización de Honeypots en redes inalámbricas es un campo relativamente nuevo que se ha estado probando con éxito en Estados Unidos [POU02]. La investigación en este tema es liderada por el programa WISE *(Wireless Information Security Experiment)* [SEC08]. En la Figura Nº14 se muestra un ejemplo del avance de las redes inalámbricas.

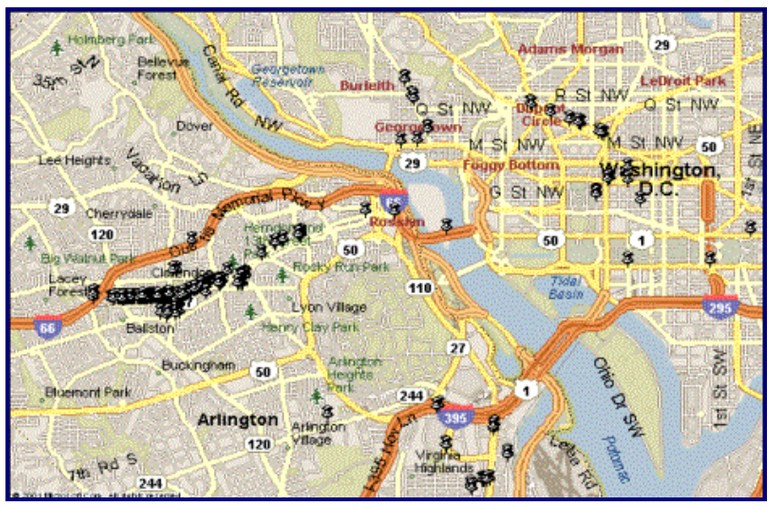


Figura Nº 14 Redes Wireless en el área de Washington D.C.

3.4 Honeynets virtuales

La disponibilidad de recursos es uno de los principales problemas a los que se ve enfrentada una organización. Por lo cual nace este tipo de Honeynet, que consiste en todos los componentes de una Honeynet normal combinados en un solo sistema, en el cual se ejecutan de modo concurrente.

Se puede definir Honeynet virtual como:

> *"la solución que permite implantar el esquema de Honeynet utilizando un único ordenador. El adjetivo virtual viene dado porque todos los sistemas operativos que existen en la Honeynet aparentemente tienen su propia máquina, aunque realmente se ejecutan en el mismo hardware."* [THE03a].

Las Honeynets virtuales pueden soportar las tecnologías GenI y GenII. Pueden clasificarse en dos grupos:

Honeynets auto-contenidas (*Self-contained* virtual Honeynet): Este tipo, abarca toda una Honeynet completa dentro de un solo sistema físico, tal como lo muestra la Figura Nº15.

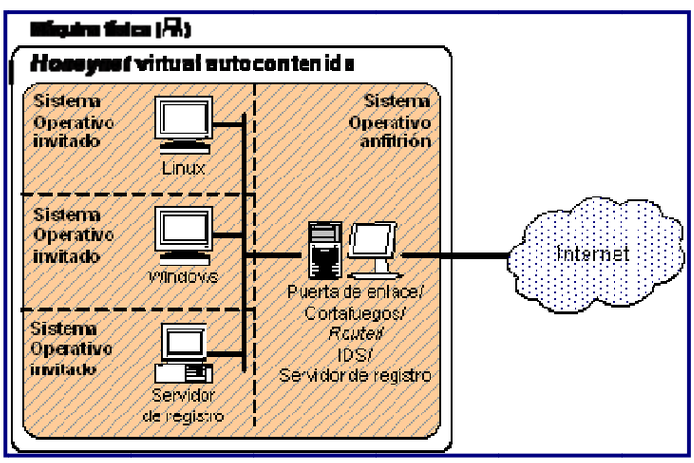


Figura Nº 15 Honeynet auto-contenida (self-contained).

La principal ventaja de este tipo de Honeynet es que sólo se necesita un computador para su funcionamiento, su rápida y fácil configuración junto con la movilidad si el equipo es un laptop. Pero esto también trae consigo desventajas. Cómo existe un solo equipo, éste tiene que ser capaz de soportar todos los equipos de la Honeynet por lo cual se requiere un equipo potente. Si el equipo llegara a fallar tanto por hardware o porque un atacante tomó el control de este, la Honeynet completa se verá afectada.

Honeypots híbridas (Hybrid virtual Honeynet): Es una combinación de equipos virtuales y reales, ya que se produce una división entre el Honeywall (punto de enlace, control y recolección de información de la Honeynet) y los Honeypots existentes, lo cual permite mitigar el riesgo. En la Figura Nº16 se puede apreciar el funcionamiento de los Honeypots híbridas.

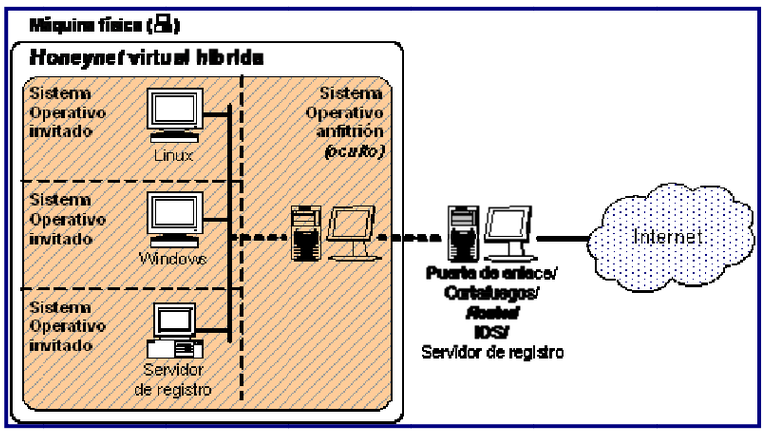


Figura Nº 16 Honeynet híbridas (Hybrid).

Con este tipo de Honeynet se gana en seguridad ya que no se tiene el riesgo de que el atacante comprometa otros equipos salvo los Honeypots. Además presenta una mayor flexibilidad a la hora de capturar y controlar la información de la red.

Sin embargo, este tipo de Honeynet también presenta ciertas desventajas. Al ser un equipo más, se pierde la movilidad en comparación a las auto-contenidas. Además incrementa el costo al tener un equipo más y su configuración es algo más compleja.

Podemos ver que ambos sistemas presentan ventajas y desventajas. Sin embargo, todo dependerá de que objetivo se persiga con la Honeynet y con cuantos recursos se cuenta a la hora de implementarla.

3.5 Honeynets Distribuidas

La idea de centralizar las distintas Honeynets permite la correlación de la información obtenida por cada nodo, así como también permite descubrir incidentes de forma más rápida y eficiente.

Se deben definir las arquitecturas a utilizar que permitan la interconexión entre los distintos sistemas. Además, se deben crear túneles privados virtuales (VPN) cifrados por ejemplo IPSec, de esta forma se conectan de manera segura al repositorio central tal como lo muestra la Figura Nº17.

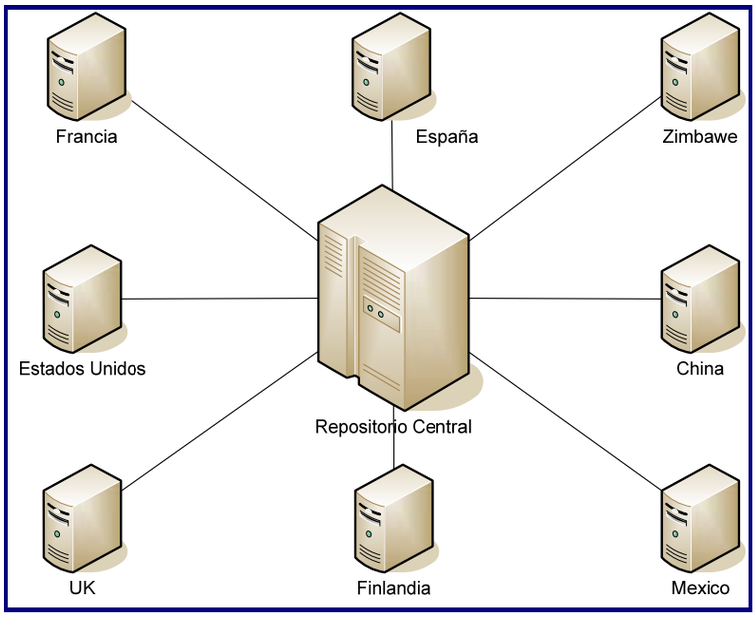


Figura Nº 17 Ejemplo Honeynets Distribuidas

Esta es una idea relativamente nueva que permitirá recolectar información a nivel mundial, con lo cual se podrán descubrir de manera mucho más rápida y eficiente los ataques realizados por la comunidad blackhat.

3.6 Resumen

En este capítulo se han detallado las tecnologías Honeypot y Honeynet, sus características, ventajas y desventajas. Así como también algunas variantes que han sufrido al complementarse con otras tecnologías como los Wireless Honeypot, Honeynet Virtuales y las Honeynet distribuidas.

De lo expresado anteriormente se pueden rescatar como se desea implementar tanto un Honeypot como una Honeynet, los objetivos para los cuales se quieren implementar y como se desea que estas tecnologías participen dentro de la organización. Es decir, si se espera que sólo protejan la red o que sirvan como un medio de investigación que traiga consigo una mejor protección y detección de ataques en la organización.

Capítulo IV DESARROLLO

Antes de comenzar con el desarrollo propiamente tal, se requiere analizar la Red del Instituto de Informática en la cual se implementará la Honeynet. Para así, poder medir el impacto que generará la incorporación de ésta en la Red del Instituto.

4.1 Red Instituto de Informática

La red del Instituto de Informática pertenece al consorcio REUNA[17] que es una iniciativa de colaboración universitaria que cuenta con la única infraestructura tecnológica de Redes Avanzadas de naturaleza académica, dedicada a la investigación y desarrollo en Chile.

La Universidad Austral de Chile pertenece a REUNA desde su creación y juntas han participado en varios proyectos de investigación y desarrollo de nuevas tecnologías.

La red del Instituto es una subred de REUNA, donde los tres primeros octetos de la dirección IP permiten identificar la red y el octeto restante es para los hosts. La red del Instituto cuenta con una dirección de red 146.83.216.128 siendo su máscara de red 255.255.255.128 o 25 en CIDR[18] (el CIDR utiliza la asignación de prefijos de longitud arbitraria lo que permite un uso más eficiente de la direcciones IPv4) con lo cual se tienen 126 hosts. Pero en realidad son sólo 125 ya que el primer hosts se utiliza como Gateway para la conexión de Internet. En la Tabla Nº5 que se muestra a continuación se puede ver más claramente lo dicho anteriormente.

Tabla Nº 5 Valores de la Red del Instituto Informática

Red	Máscara	Host Min	Host Max	Broadcast	Host/ Red
146.83.216.128	255.255.255.128	146.83.216.129	146.83.216.254	146.83.216.255	126

Además, la red presenta dos servidores primordiales, estos son el 146.83.216.201 y el 146.83.216.209. Donde el primero es el servidor DNS primario del Instituto, mientras el segundo se encarga de dar DHCP y también es el servidor DNS secundario de la red.

A continuación, la Figura Nº18 presenta un esquema donde se puede apreciar claramente el funcionamiento de la red del Instituto, los servidores principales y cómo los servicios prestados por estos son utilizados en los distintos laboratorios del Instituto.

[17] Red Universitaria Nacional http://www.reuna.cl
[18] Classless Inter-Domain Routing

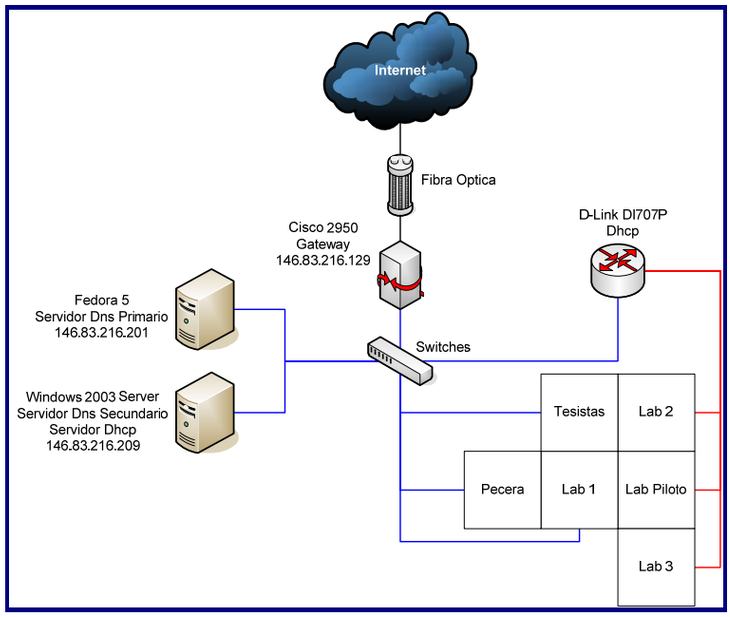


Figura Nº 18 Esquema Red Instituto Informática

Las líneas azules del esquema anterior representan la red pública del Instituto, esto quiere decir, que se utilizan las IP de la red 146.83.216.128. Las líneas rojas en cambio representan IP privadas generadas por el router D-Link DI707P, los laboratorios a los cuales este router les entrega dichas IP pueden variar dependiendo del uso que se le da al laboratorio. Un ejemplo de esto es la utilización del laboratorio tres en el segundo semestre en la asignatura de Taller de Ingeniería de Software, donde éste es conectado a la red pública del Instituto. En la Figura Nº19 se presenta un esquema en forma de plano, de la distribución de los laboratorios del Instituto en el cuál se puede observar la distribución de los elementos de cada laboratorio y del espacio físico que utilizan.

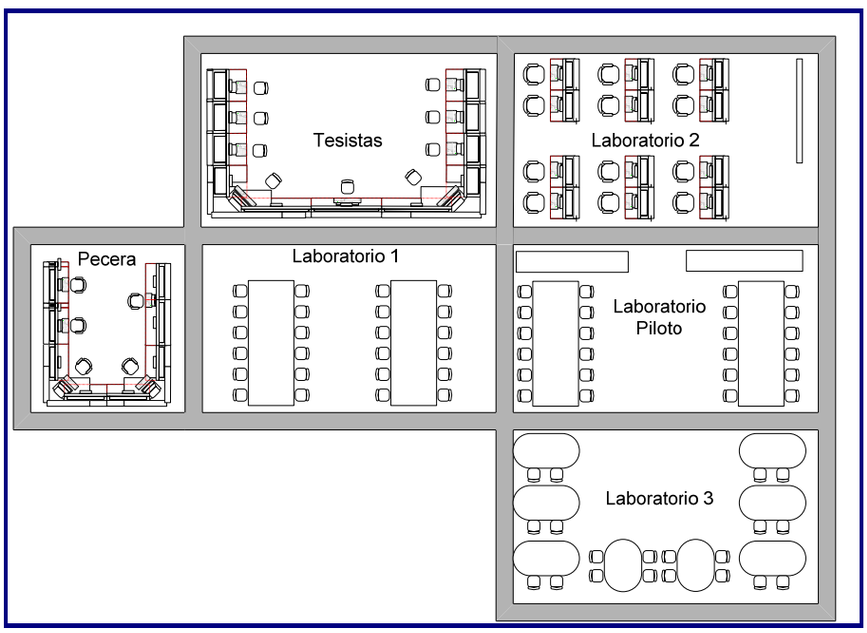


Figura Nº 19 Esquema laboratorios Instituto

4.2 Diseño de una Honeynet en la Red del Instituto

Al analizar la red del Instituto se puede apreciar que existen dos posibilidades para incluir una Honeynet. En la Figura Nº20 se muestran estas dos posibilidades.

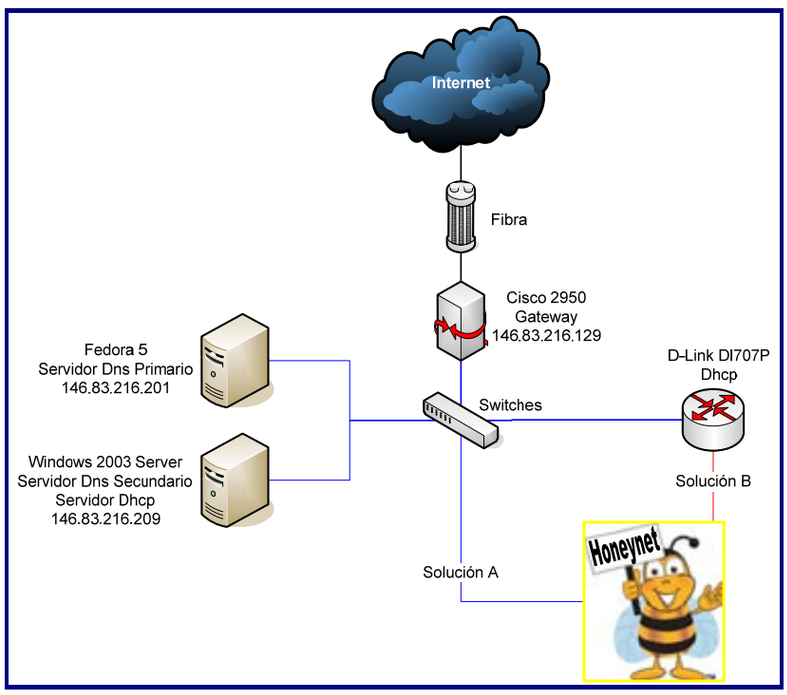


Figura Nº 20 Posibles Honeynet en el Instituto

En el esquema aparecen las dos posibles soluciones llamadas Solución A y B. La solución A consta de una red pública y está conectada directamente a los servidores del Instituto. La solución B en cambio está conectada a la red privada del Instituto y por ende está alejada, por lo que una implementación en esta red perdería la importancia que se le quiere dar a la Honeynet ya que ningún servidor estaría relacionado con los Honeypots lo que hace más fácil su detección y disminuye el interés del atacante. Por este motivo se desestimó la solución B y se implementará la solución A.

Tomando en cuenta lo que se presentó en el capitulo anterior se puede ver que hay distintas formas de implementar una Honeynet y este caso no es distinto. Dada la red que presenta el Instituto de Informática se podrían implementar tres tipos de Honeynet, la primera con equipos virtuales, la segunda con un modelo hibrido y la tercera con equipos físicos.

La primera opción se descartó por no contar con los recursos necesarios para dicha implementación, ya que se necesita un equipo realmente potente para poder implementar los Honeypots y el Honeywall.

La segunda opción era el modelo híbrido, donde un equipo realiza la labor de Honeywall y el otro tiene los Honeypots implementados como maquinas virtuales dentro. En la Figura Nº21 se puede apreciar cómo sería la implementación de dicha opción.

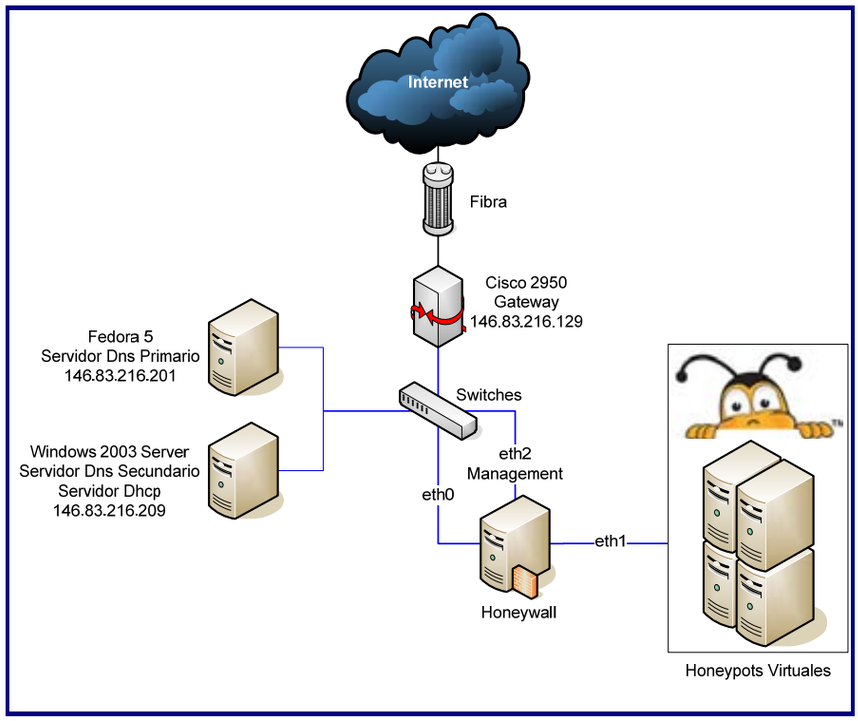


Figura Nº 21 Posible Implementación modelo híbrido

Como se puede observar en el modelo anterior, para poder implantar esta opción es necesario constar con un equipo relativamente poderoso para que contenga virtualmente a los Honeypots y como el fin de esta Tesis es utilizar los equipos que están en desuso en los laboratorios se desechó por necesitar un presupuesto relativamente alto.

La última opción, de utilizar equipos físicos fue la que se decidió utilizar ya que así, se le daría un nuevo uso a los equipos que no estaban siendo utilizados con lo cual no fue necesario contar con un gran presupuesto para desarrollar este proyecto junto con ahorrar en la compra de equipos de última generación.

Dentro de esta opción a implementar, todo dependerá del diseño de red que se quiera implementar y que mejor se acomode a la realidad del Instituto. Para esto se estudiaron dos tipos de esquemas los cuales se pueden apreciar a continuación en las Figuras Nº22 y Nº23.

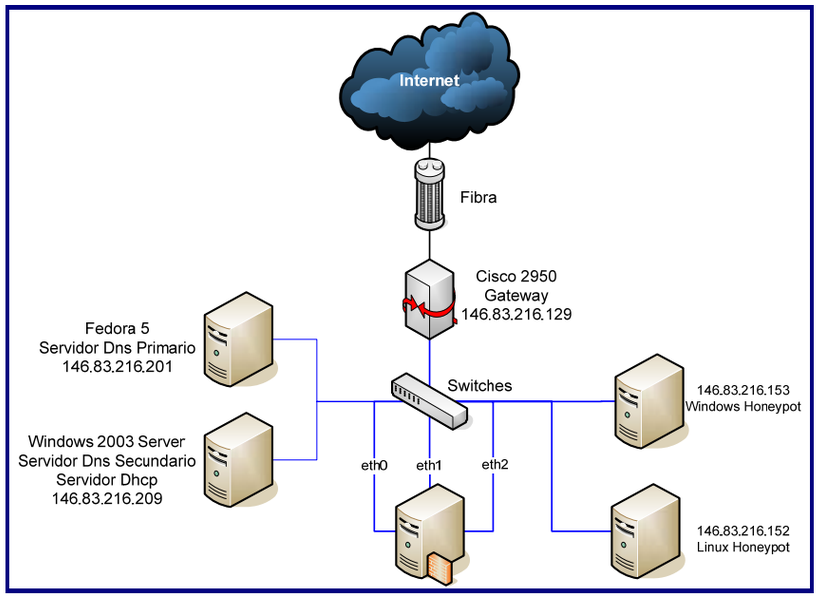


Figura Nº 22 Esquema red físico 1

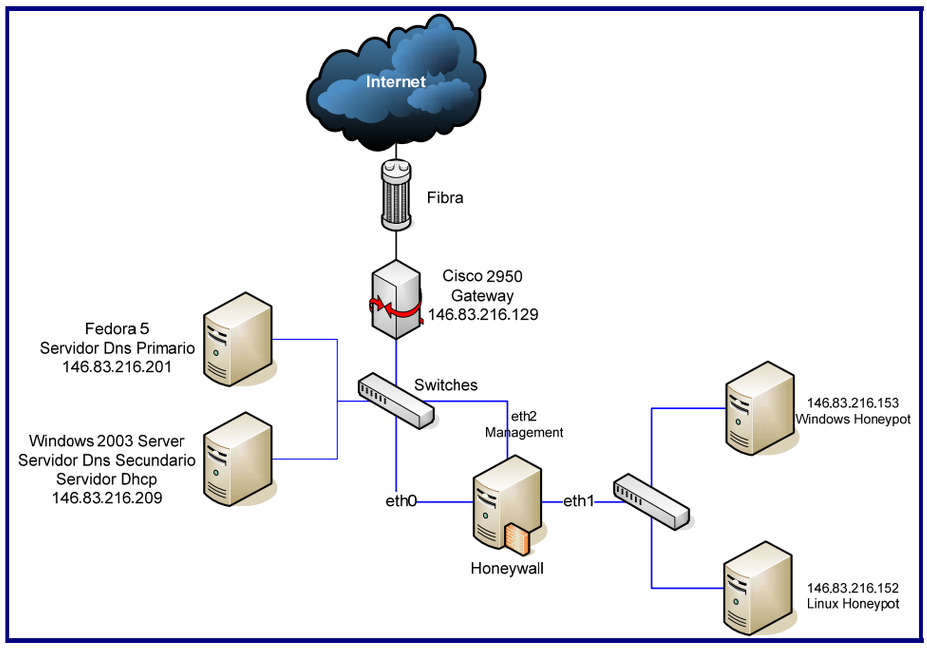


Figura Nº 23 Esquema red físico 2

Como se puede apreciar en los esquemas anteriores, estos presentan algunas similitudes como por ejemplo que ambos están conectados a la red pública del Instituto. Su diferencia radica principalmente en que el esquema 1 tiene todos los equipos conectados directamente a los switchs del Instituto, mientras que en el esquema 2 los Honeypots están conectados al Honeywall y éste a su vez a algún switch del Instituto.

Esta diferencia, aunque no parezca relativamente importante, es todo lo contrario. El esquema 1 con los Honeypots conectados directamente a los switchs del Instituto podría provocar una posible saturación de la red al estar el Honeywall revisando todos los paquetes que atraviesan los switchs del Instituto que se dirigen a los Honeypots.

Además, algunos paquetes dirigidos a los Honeypots podrían no ser registrados por el Honeywall. En cambio, en la segunda opción el Honeywall sólo se encarga de vigilar el tráfico hacia los Honeypots y al estar conectados detrás de él todo el tráfico dirigido hacia estos es registrado.

Por este motivo se prefiere utilizar la segunda opción para así no perjudicar la red del Instituto y no perder datos importantes, que son el objetivo principal de este proyecto haciendo mucho más confiable la Honeynet a implantar.

4.3 Implementación de la Honeynet en la Red del Instituto

Para realizar la implementación, se utiliza la siguiente pauta realizando las tareas que aquí se describen. El fin de esto, es tener claro que se debe realizar para obtener una correcta implementación de la Honeynet.

1. Seleccionar los equipos a utilizar.
2. Instalar, Configurar y Actualizar los Sistemas Operativos a los equipos Honeypot.
3. Instalar y Configurar los servicios en los equipos Honeypot.
4. Probar el correcto funcionamiento de los servicios.
5. Instalar y Configurar el equipo Honeywall.
6. Probar el correcto funcionamiento de la Honeynet.

Como se vio en el punto anterior la idea es conectar la Honeynet a implementar a algún switch de la red pública de la red del Instituto. Además se pretende utilizar dos equipos como Honeypot, el primero utilizando un Sistema Operativo Linux y el segundo utilizando el Sistema Operativo Windows 2003 Server, la idea es tener sistema representativos de la red. El Sistema Linux a utilizar es Gentoo Linux, debido a su gran documentación, además de estar presente en la red de la Facultad de Ingeniería en la cual se encuentra el Instituto de Informática. En este sistema se pretende dar los servicios más comunes como Web, FTP, DNS, Mail, Proxy y disponer de una Base de Datos como Oracle 10g Express para ello se dispuso de un equipo con las siguientes características. Un equipo marca Compaq Deskpro EN con un procesador Pentium III de 866Mhz con 512Mb en memoria y 40Gb de disco duro.

El equipo con Windows 2003 Server constará con los servicios Web, FTP, DNS, File Server para esto se dispuso de un equipo con las siguientes características. Es un equipo marca Compaq Deskpro EN con un procesador Pentium III de 866Mhz con 512Mb en memoria y 40Gb de disco duro.

Para implementar el Honeywall se utilizó un equipo un poco más potente ya que éste equipo es el que se lleva todo el trabajo. Por ello el equipo utilizado cuenta con las siguientes características, un procesador Pentium IV de 1800Mhz con 1Gb de memoria y 80Gb de disco duro.

A continuación, en la Figura Nº24 se puede observar un esquema de los equipos utilizados, los servicios que estos proveen, y como se comunican con otros servidores como el DNS del Instituto y el servidor del Servicio Hidrográfico y Oceanográfico de la Armada de Chile. Con este último los tres equipos están conectados para mantener sus relojes sincronizados con la hora oficial del país.

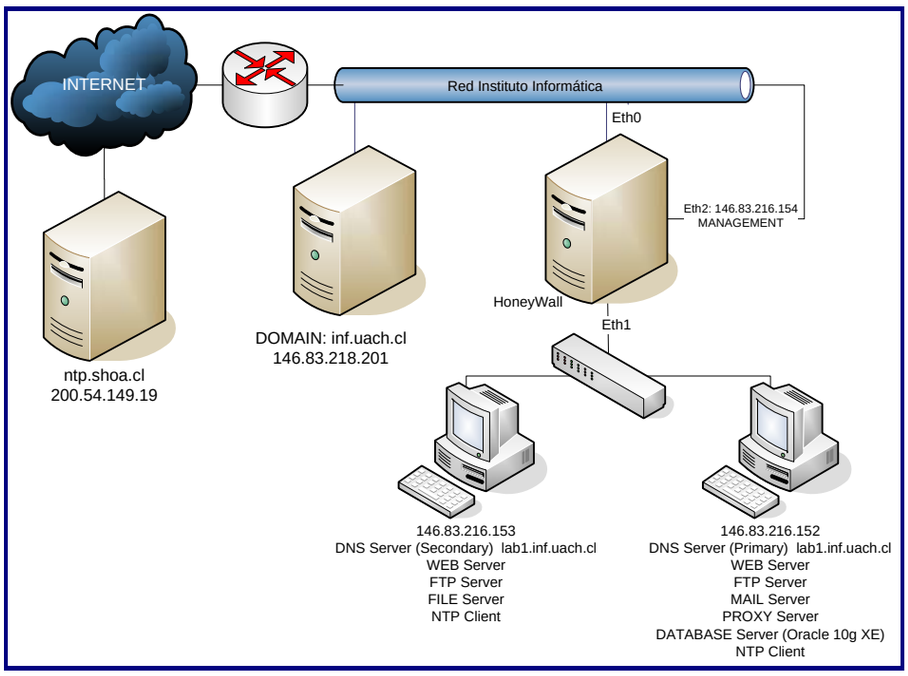


Figura Nº 24 Esquema a implementar en la red del Instituto

4.3.1 Implementación Gentoo Server

Para la instalación del Sistema Operativo Gentoo se utilizó la versión 2005.1 siendo de gran utilidad el Gentoo Handbook para esa versión [GEN05] y el Handbook para la última versión la 2008.0 [GEN08a]. Se escogió la versión 2005.1 ya que ésta permite instalar el Sistema Operativo por línea de comandos junto con permitir compilar el kernel para ajustarlo óptimamente al hardware del equipo. Las versiones más nuevas en

cambio, se instalan al igual que cualquier otra distribución de Linux a partir de un Live CD con la mayor parte del sistema pre-compilado. Como el equipo en el cual se instalará no es un equipo relativamente nuevo se prefirió la versión más antigua y una vez instalado el Sistema Operativo compilado óptimamente con el hardware del equipo se dispuso a actualizarlo completamente.

Para actualizar correctamente el sistema es necesario actualizar primero el Portage. El Portage es un árbol que contiene toda la información de las aplicaciones estables para este sistema operativo. Para actualizarlo se ejecuta el siguiente comando.

```
#emerge --sync
```

Ahora que se ha actualizado el Portage lo siguiente es actualizar el sistema completamente mediante la siguiente instrucción

```
#emerge --update --deep --newuse world
```

Una vez actualizado el sistema se dispuso a instalar los softwares que permitirán ofrecer distintos tipos de servicios al Servidor Gentoo. Como se puede observar con los comandos anteriores para instalar algún software en necesario utilizar el comando *emerge* el cual baja, compila e instala el software, para mayor información dirigirse a las referencias [GEN08b].

El primer servicio que se levantó fue el HTTP Server para lo cual fue necesario instalar el servidor Apache mediante el comando *emerge apache*, luego se procedió a revisar los archivos de configuración y a cargar una página de muestra. En Configuración_Apache que se encuentra en el Anexo B.3 se puede observar los archivos de configuración de apache y la página Web funcionando en el Servidor.

A continuación se dispuso a instalar y configurar un servidor FTP para ello se utilizó el software PureFTP ya que es mucho más seguro que el FTP por defecto ProFTP. Para esto, se siguió la guía que aparece en el Anexo B.3 Configuración_PureFTP, en ella se puede observar paso a paso la forma de configurarlo y además, se encuentra el archivo de configuración que está funcionando en el servidor.

En las Figuras Nº25 y Nº26 que se encuentran a continuación se puede observar los servicios descritos anteriormente, configurados y funcionando correctamente.

Figura Nº 25 Servidor Web funcionando

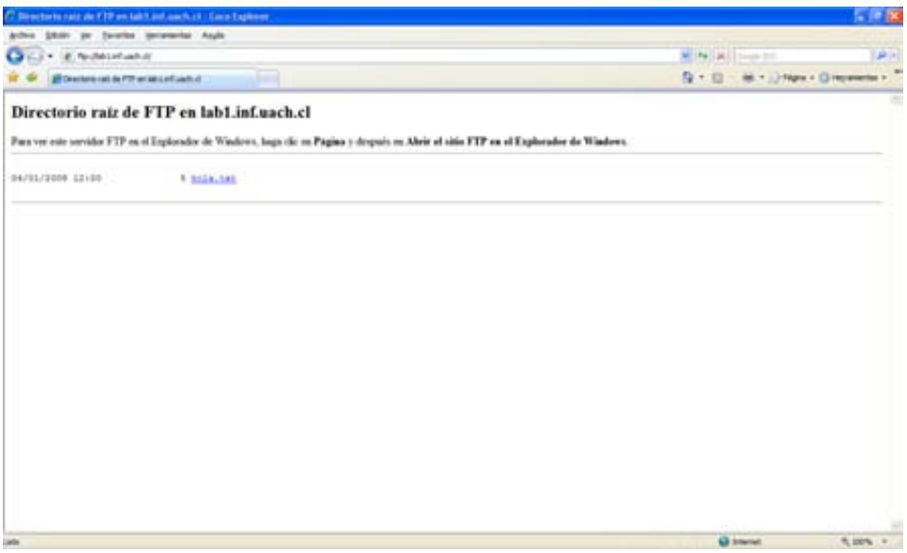


Figura Nº 26 Servidor FTP funcionando

Luego se dispuso a instalar y configurar un servidor Proxy, para esto se utilizó el software Squid por ser el más versátil del mercado. Para configurarlo se utilizó la guía que se encuentra en el Anexo B.3 Configuración_Squid y el documento "Administración y Seguridad en Linux" del curso del mismo nombre dictado por Daniel Eugenin. En el Anexo, además se encuentran los archivos de configuración utilizados en el servidor.

Para constar con una Base de Datos se utilizó Oracle 10g Express por ser gratuita y por estar dentro de las más utilizadas. Para la configuración de ésta se utilizó la guía del Anexo B.3 Configuración_Oracle, en la cual se puede observar claramente como instalar y configurar la Base de Datos. Además, se incluyó los archivos de configuración utilizados en el servidor. A continuación, en las Figuras Nº27 y Nº28 se puede observar la base de datos configurada y funcionando correctamente en el servidor.

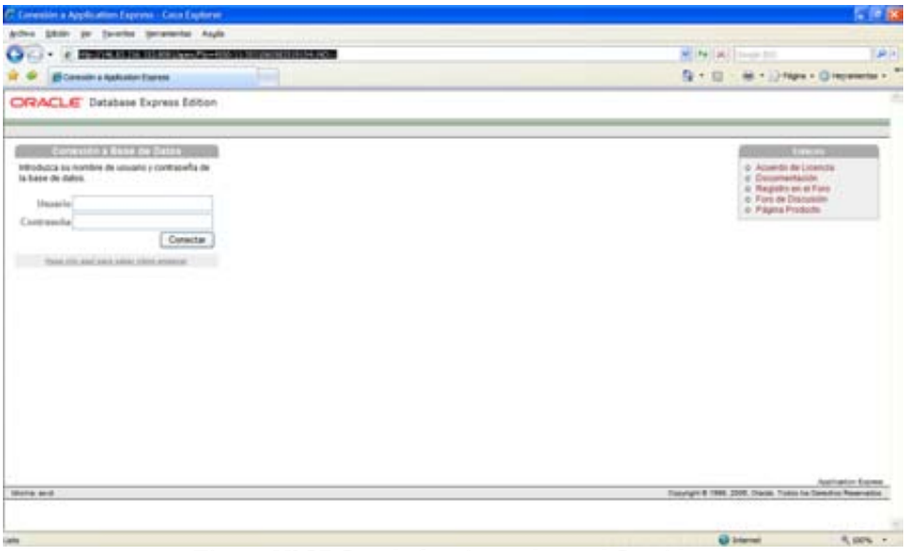


Figura Nº 27 Oracle funcionando en el Servidor

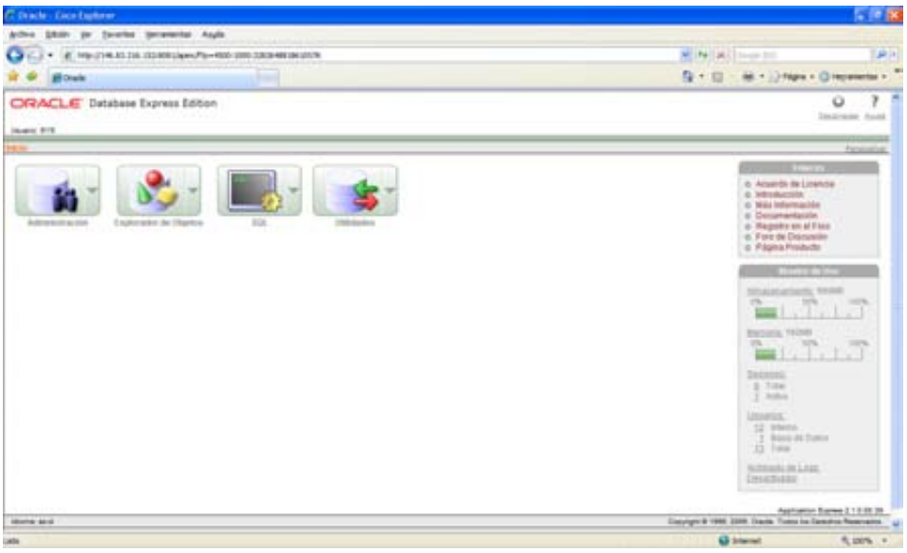


Figura Nº 28 Sistema de Administración de Oracle

Lo siguiente fue configurarlo como un Servidor DNS para lo cual se siguió la guía que aparece en el Anexo B.3 Configuración_DNS. Además, se incluyen los archivos de configuración y zonas del servidor junto al del Servidor del Instituto.

Lo primero en realizar, fue agregar el equipo como un servidor DNS dentro del servidor DNS del Instituto. Para esto, se modificó el archivo /etc/named.conf agregando el servidor como se ve a continuación.

Listado de Código: /etc/named.conf

```
zone "inf.uach.cl" IN {
        type master;
        file "inf.uach.cl.zone";
        notify yes;
        allow-transfer { 146.83.216.4; 200.2.114.138; 146.83.216.209;
146.83.216.152; 146.83.216.250; };
};
```

Esto permite que el Servidor del Instituto le envíe la zona inf.uach.cl al servidor Gentoo. Además se modificó el archivo de zona para que reconociera al servidor Gentoo como servidor DNS de una zona interna llamada lab1.inf.uach.cl. Para lograr esto, es necesario agregar las siguientes líneas al archivo de zona del servidor DNS del Instituto.

Listado de Código: archivo de zona inf.uach.cl

```
lab1            1D IN NS        ns.lab1
ns.lab1         1D IN A         146.83.216.152
```

Finalmente se instaló y configuró un servidor de correos virtual con Postfix para ello se utilizó la guía que se encuentra en el Anexo B.3 Configuración_Correo en la cual también se encuentran los archivos de configuración implementados en el Servidor. Esta guía está bien detallada y se explica paso a paso como configurar el Servidor de correos y como ir agregando distintas funcionalidades a este.

A continuación, en la Figura Nº29 se puede observar la interfaz Web del sistema de correo funcionando correctamente en el servidor.

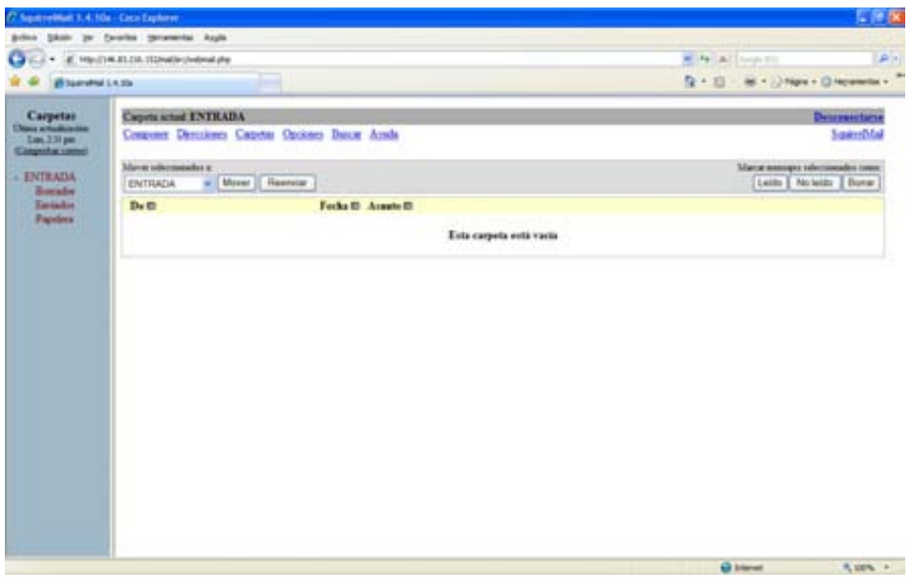


Figura Nº 29 Cuenta de Correo en el Servidor Gentoo

Todos estos servicios se encuentran funcionando en el equipo Servidor Gentoo que se encuentra en el laboratorio de Tesistas con la IP 146.83.216.152.

4.3.2 Implementación Windows Server

Para la implementación del Servidor Windows, se utilizó la versión Windows 2003 Enterprise Server, su instalación se hizo como cualquier equipo Windows salvo por la configuración de licencias la cual permite atender cierto número de conexiones al servidor. Como se puede observar en la Figura_B73 se utilizó la configuración por dispositivo la cual permite tener un mayor número de conexiones en el Servidor según lo que soporte el dispositivo.

Una vez instalado el Sistema Operativo, se dio paso a instalar los servicios destinados a este equipo mediante la aplicación Administre su Servidor. Lo primero fue instalar un Servidor de Aplicaciones para ofrecer servicios Web, para una vista detallada de lo que se debe realizar visitar el Anexo B.2 Servidor Windows desde la Figura_B75 a la Figura_B78.

Luego, se le agregó un FTP para que el servidor de aplicaciones conste con este componente. Esto se puede observar claramente desde la Figura_B79 a la Figura_B82 del Anexo B.2 Servidor Windows. Una vez instaladas ambas funciones se debe acceder a la Administración de ambos para configurarlos como se puede apreciar claramente desde la Figura_B83 a la Figura_B90 del mismo Anexo citado.

Como se puede observar claramente en las Figuras descritas anteriormente una vez configurado el servidor éste queda habilitado inmediatamente para su funcionamiento cómo se puede apreciar en las Figuras Nº30 y Nº31.

Figura Nº 30 Página Web funcionando en Servidor Windows

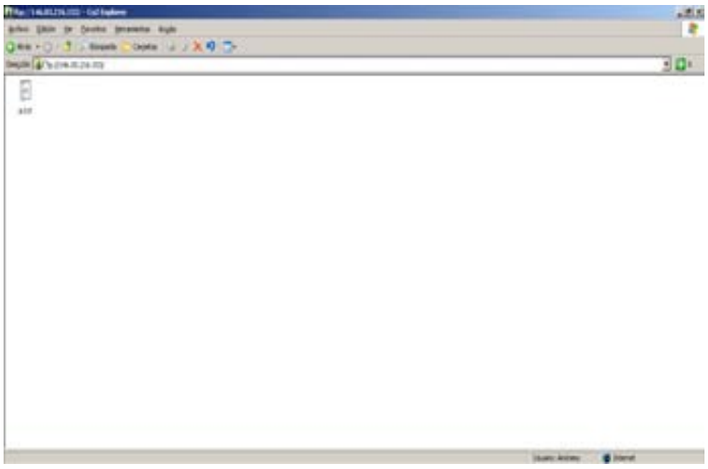


Figura Nº 31 FTP funcionando en Servidor Windows

A continuación se instaló y configuró un Servidor de Archivos el cual permite traspasar archivos entre distintos equipos, la instalación y configuración de éste se puede observar claramente desde la Figura_B91 a la Figura_B99 del Anexo B.2 Servidor Windows. Como se puede apreciar en las figuras, se debe configurar la carpeta en la cual se encontraran los archivos, junto con los permisos de ésta. Una vez finalizado los pasos de configuración el servidor ya está disponible para ofrecer este servicio.

Lo siguiente fue instalar y configurar el servidor DNS, esto se puede apreciar detalladamente desde la Figura_B100 a la Figura_B114 del Anexo B.2 Servidor Windows. Como se puede apreciar en las figuras, el servidor fue configurado como servidor secundario del servidor Gentoo del cuál obtiene los archivos de zonas.

En la Figura Nº32 se puede observar al Servidor Windows funcionando correctamente como servidor DNS Secundario de la zona lab1.inf.uach.cl

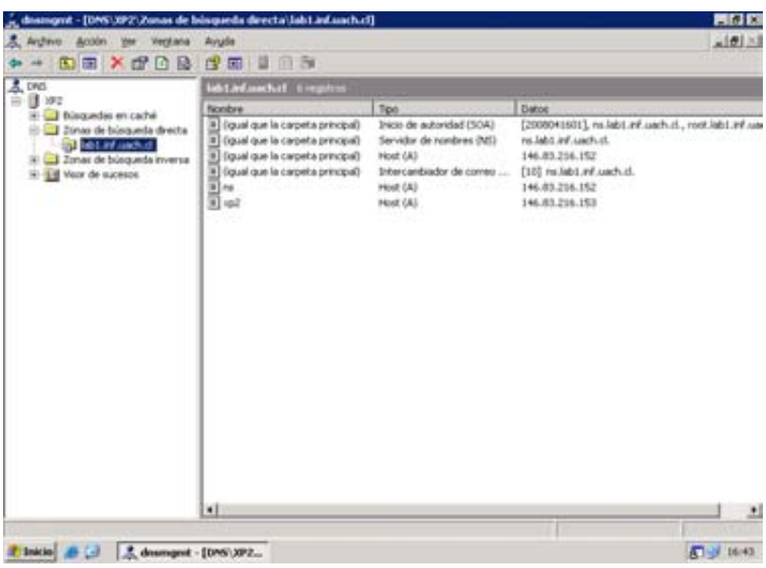


Figura Nº 32 Servidor DNS funcionando en Servidor Windows

Todos estos servicios se encuentran funcionando en el equipo Servidor Windows que se encuentra en el laboratorio de Tesistas con la IP 146.83.216.153.

4.3.3 Implementación Honeywall

Para la implementación del Servidor Honeywall se utilizó en una primera etapa la versión Roo 1.2 ya que ésta era la versión más actual al momento de la instalación. Ésta instalación sirvió como prueba para comprender el funcionamiento de dicha distribución, ya que en marzo de 2008 apareció la nueva versión estable llamada Roo 1.4 que es la usada actualmente. Todos los pasos que se describirán a continuación pueden observarse claramente en el Anexo B.1 Servidor Honeywall

Su instalación es relativamente sencilla, ya que sólo se debe arrancar el equipo con el cdrom y aparecerá la pantalla que se muestra en la Figura Nº33.

Figura Nº 33 Inicio instalación Honeywall

Como se puede apreciar en la figura anterior, sólo basta presionar Enter para comenzar la instalación, la cual sobrescribirá todos los datos del disco duro del equipo. A continuación se puede observar el proceso de instalación del equipo en la Figura Nº34.

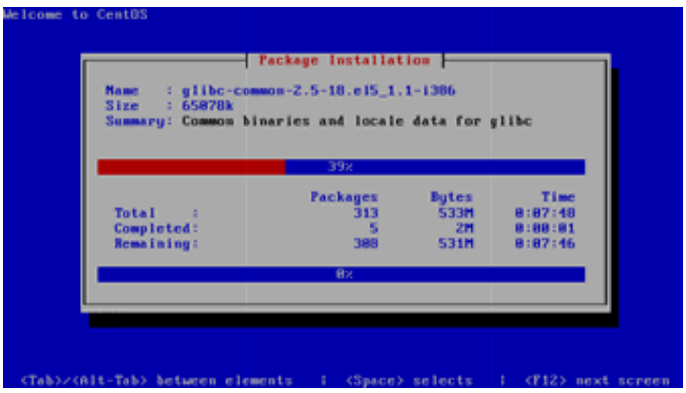


Figura Nº 34 Instalación Honeywall

Una vez finalizada la instalación el equipo reiniciará y aparecerá la pantalla que se describe en la Figura Nº35.

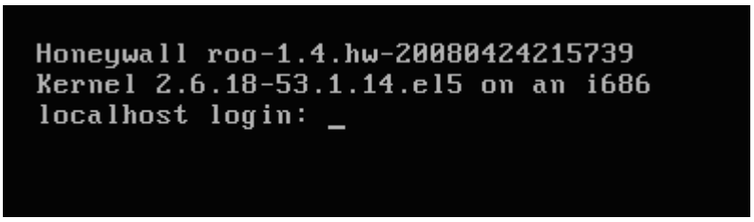


Figura Nº 35 Honeywall instalado

El equipo ha sido instalado con la nueva versión de Honeywall la cual está desarrollada bajo CentOS. El Honeywall por defecto viene con 2 usuarios de sistema que son roo y root, ambos usuarios vienen por defecto con la password honey. No se puede ingresar directamente como usuario root, sino que para iniciar sesión primero se deberá ingresar como el usuario roo y ejecutar el comando su – para tener acceso a root.

Una vez que se haya ingresado como usuario root aparecerá el primer mensaje el cuál dice que el Honeywall aún no ha sido configurado y que se procederá a mostrar el menú de configuración. Si por algún motivo saliera del menú de configuración sólo basta escribir menú en la consola para volver al menú de configuración.

En la Figura Nº36 se puede apreciar el menú de configuración y las opciones que contiene.

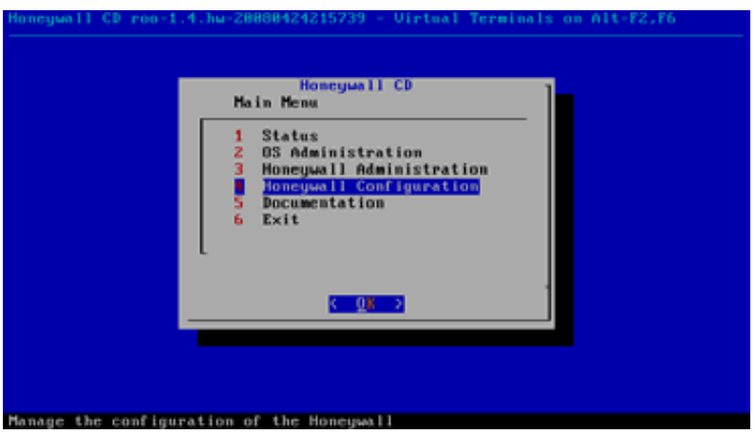


Figura Nº 36 Menú configuración Honeywall

Ahora se procederá a realizar la parte fundamental que es la configuración del Honeywall, la cual permitirá monitorear los Servidores que se han configurado anteriormente.

Para ello se debe escoger la opción número cuatro del menú que dice Honeywall Configuration. En seguida, aparecerá un mensaje que habla sobre la limitación de responsabilidad, en este mensaje aparecen los riegos que trae instalar una Honeynet y si estamos dispuestos a aceptarlos, seleccionamos yes y presionamos enter.

La siguiente ventana preguntará que método se utilizará para la instalación, esta puede ser mediante un diskette con el archivo honeywall.conf previamente cargado en él, con una configuración por defecto o mediante una entrevista. Esta última opción permite ir ingresando los valores que se desean utilizar contestando las preguntas que van apareciendo en pantalla. En la Figura Nº37 que se muestra a continuación, se puede apreciar lo dicho anteriormente.

Figura Nº 37 Métodos de configuración del Honeywall

Por no contar con otros Honeywall instalados como para utilizar la configuración de ellos, se elegirá la opción de entrevista en vez de la opción del diskette, ya que así se irá definiendo paso a paso la configuración acorde al estudio realizado sobre la red del Instituto.

En la primera etapa de configuración, se deberá ingresar las IP que tendrán los equipos Honeypot que para este caso serán 146.83.216.152 y 146.83.216.153, la red en la cual se encuentran los Honeypots que en este caso es 146.83.216.128/25 y la dirección de Broadcast de los Honeypot que en este caso es 146.83.216.255. Todo esto se puede apreciar más claramente desde la Figura_B12 a la Figura_B16 del Anexo B.1.

La segunda etapa consiste en configurar el nombre del equipo y el dispositivo de administración remota. Para ello se deberán ingresar los campos correspondientes como la IP de administración del equipo que en este caso es 146.83.216.154, su máscara 255.255.255.128, el Gateway 146.83.216.129 y el DNS 146.83.216.201. También, se debe configurar el acceso externo al equipo mediante SSH, donde se preguntará si

permite el acceso al usuario root, con ello, se pedirá un cambio de password para los usuarios del sistema, y además se pedirá los puertos a los cuales permitirá conexión el servidor tanto TCP como UDP. Todo esto se puede apreciar más claramente desde la Figura_B17 a la Figura_B44 del Anexo B.1.

La tercera etapa consiste en configurar la cantidad de conexiones de salida permitidas para los distintos tipos de protocolos como ICMP, TCP, UDP y otros. Además, se habilitará el IPS y se configuraran los archivos para la captura de datos. Todo esto se puede apreciar más detalladamente desde la Figura_B45 a la Figura_B58 del Anexo B.1.

La cuarta etapa consiste en configurar la actividad que los Honeypot tendrán con los equipos DNS y cómo será el acceso entre ellos. En este caso el equipo DNS al cual tendrán acceso los Honeypot es el equipo 146.83.216.201. Esta configuración se puede apreciar más claramente desde la Figura_B59 a la Figura_B63 del Anexo B.1.

La quinta y última etapa de configuración consiste en configurar los mecanismos de alerta como por ejemplo un correo electrónico donde se reciban las alertas generadas por el servidor y la configuración de las variables del sistema Sebek el cual permite realizar la captura de Datos. Esto se puede apreciar más claramente desde la Figura_B64 a la Figura_B71 del Anexo B.1.

Con esto el equipo ya cuenta con la configuración básica para el correcto funcionamiento dentro de la red del Instituto. El paso siguiente es configurar el Walleye o Honeywall Web Interface, para que pueda funcionar. Para ello es necesario generar un certificado SSL y una KEY. Esto se puede realizar utilizando los comandos que aparecen a continuación y una vez ejecutados se debe reiniciar el webserver.

```
#/usr/bin/openssl genrsa 1024 > /etc/walleye/server.key

#/usr/bin/chmod go-rwx /etc/walleye/server.key

#/usr/bin/openssl req -new -key /etc/walleye/server.key -x509 -days 365
-out /etc/walleye/server.crt

#/usr/bin/openssl x509 -noout -fingerprint -text <
/etc/walleye/server.crt

#/etc/init.d/walleye-httpd restart
```

Lo siguiente es habilitar Walleye, esto se realiza desde el menú en la opción "4: Honeywall Configuration", luego "2: Remote Management" y finalmente "12: Walleye" y habilitarlo. Una vez activo y funcionando correctamente se puede acceder a él mediante algún Browser digitando https://ip-address-mgmt-interface que en este caso sería https://146.83.216.154/. En la Figura Nº38 se puede apreciar el Walleye funcionando correctamente en el Honeywall.

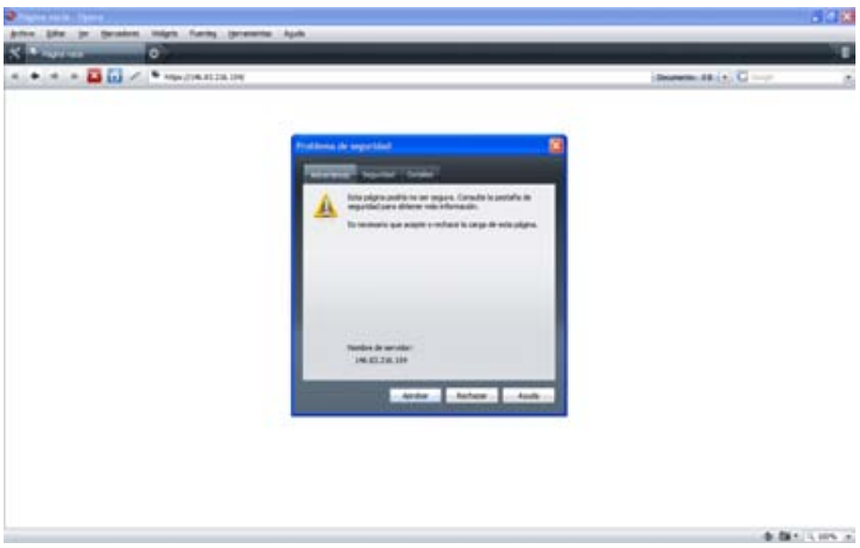


Figura Nº 38 Certificado del Honeywall

Como se puede apreciar en la figura anterior lo primero que aparecerá será el certificado creado anteriormente y para ingresar a la página de Administración se debe aceptar este certificado. Una vez aceptado el certificado aparecerá la pantalla inicial del Honeywall, como se puede apreciar en la Figura Nº39.

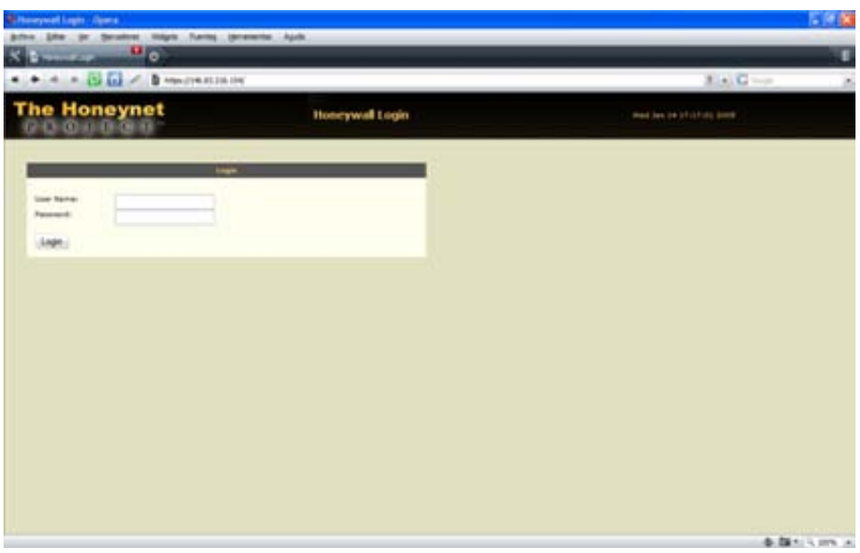


Figura Nº 39 Página de inicio Honeywall

Para ingresar al Walleye es necesario ingresar como usuario roo y password honey e inmediatamente el sistema pedirá un cambio de password donde esta debe tener al menos 8 caracteres donde uno debe ser un número, uno un carácter con letra mayúscula y uno debe ser un símbolo. Una vez finalizado esto, se ingresa a la pantalla principal como se puede apreciar en la Figura Nº40.

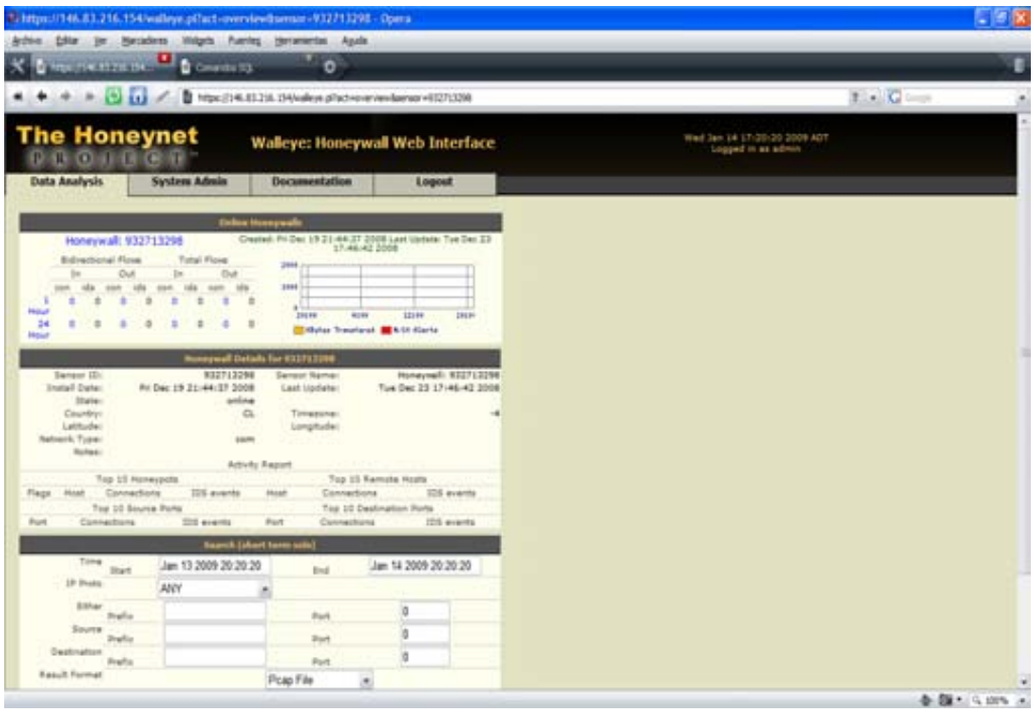


Figura Nº 40 Página principal del Honeywall

Ahora que el sistema se encuentra funcionando sólo resta actualizar las reglas del IDS e IPS. Para realizar esto, lo primero es registrarse en la página Web de Snort http://www.snort.org, una vez registrado se debe acceder a la cuenta de Snort y ver el *oink code* generado para este usuario. Una vez obtenido el *oink code*, lo siguiente es ir a la opción de actualizar estas reglas, este proceso se puede realizar de dos formas.

La primera forma y la más sencilla es ingresar mediante la interfaz Web, ingresando en "System Admin" y seguidamente ingresar en "Snort rules Management" una vez ahí se debe escribir el *oink code* obtenido de la cuenta Snort y se deben elegir los valores que sean necesarios, así como el día y la hora para que se realice este procedimiento automáticamente. En la Figura Nº41 se puede apreciar más claramente como se realiza este procedimiento.

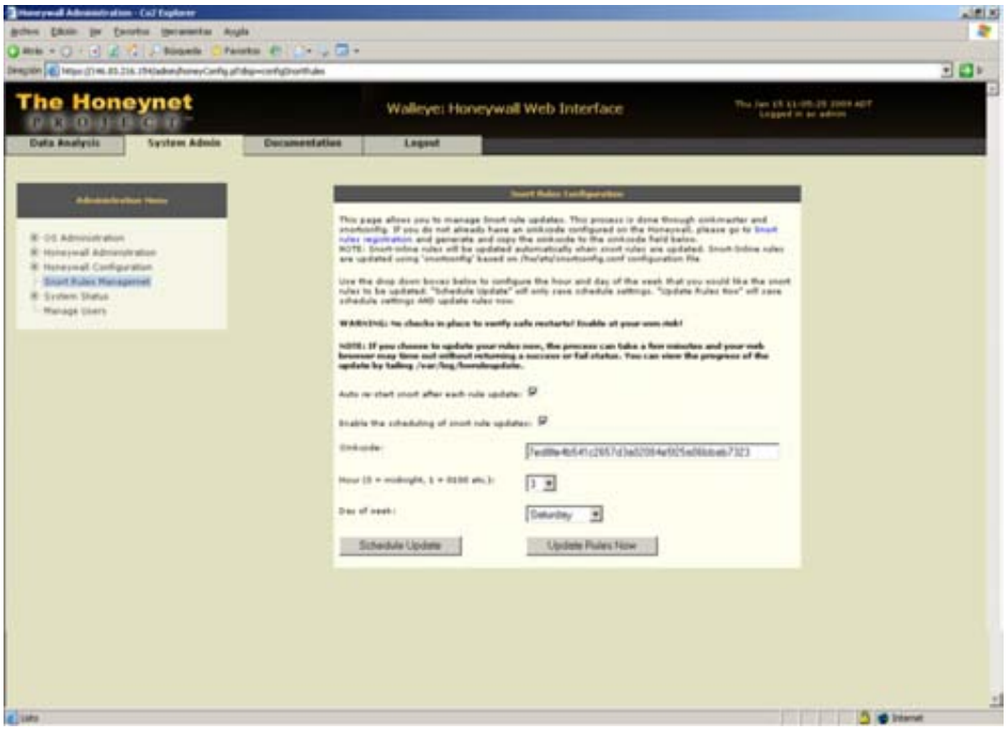


Figura Nº 41 Actualización de las Reglas de Snort

La segunda forma es acceder al menú de configuración de la consola, entrando a "Honeywall Configuration" luego a "13 Snort Rule Updates" y finalmente a "1 Configure Rule Updates". Una vez aquí, se realizan los mismos pasos que se vieron para la interfaz Web, como ingresar el *oink code*, el día y la hora de la actualización y si se desea que snort y snort-inline se reinicien después de la actualización.

Con este último paso el sistema Honeywall está finalmente instalado, su funcionamiento es relativamente intuitivo y mediante su interfaz Web se pueden realizar la mayoría de acciones relativas a la administración del Sistema haciendo estos procedimientos mucho más sencillos y simples.

Al ingresar por primera vez a la interfaz Web, ésta ingresará a la sección de Análisis de Datos, más específicamente al resumen del análisis que es un resumen de la actividad capturada por el Honeywall. Dentro de esta página, esta la sección del sensor, la cual ofrece una panorama general de lo percibido por el Honeywall. La identificación del sensor se basa en la gestión de dirección IP del Honeywall. Si se cambia la dirección IP del Honeywall, se tendrá múltiples sensores listados.

El propósito de la página de resumen es dar una visión general de la actividad del Honeywall. Los datos desplegados son una combinación de datos de Snort y Argus donde son agrupados como flujos entrantes y salientes. La principal fuente de información es el flujo de información de Argus.

Dentro de los flujos existe también el flujo bidireccional, este se define como cualquier flujo de datos que se envía en ambos sentidos: del cliente al servidor y servidor a cliente. El total incluye tanto flujos bidireccionales como unidireccionales. Además, muestra alertas de IDS y el tráfico de la red.

La sección de detalle del sensor proporciona un resumen de los datos administrativos del Honeywall, donde uno de los principales informes es aquel que habla de las últimas 24 horas. El resumen administrativo está dirigido a entornos distribuidos y proporciona una descripción de la ubicación geográfica y la organización del Honeywall. La parte superior de ésta, muestra los informes de los 25 hosts más activos y los destinos de las conexiones de red.

Al hacer clic en la sección de conexión, aparecerá el flujo de dicha conexión, ahora si el clic lo realiza sobre algún evento IDS, este le llevará a los flujos relacionados con el evento IDS y si realiza el clic sobre la dirección IP del host, este le llevará a una página resumen sobre el Host.

El final del menú es para consultar la información basada en una IP específica. Es relativamente auto-explicativo, permite buscar sobre alguna hora o fecha específica, la dirección IP y / o puertos.

La sección de Flujos es aquella donde se puede ver un resumen de todas las conexiones entrantes y salientes relacionadas con alguna actividad. En esta sección aparecerá la información ordenada por Honeypot (por IP), pero puede ser ordenada por cualquiera de las otras cabeceras que allí aparecen. En la parte inferior izquierda aparece la opción de consultar por flujos específicos, las opciones de consulta pueden ser el filtrado por tipo de trafico ya sea unidireccional como bidireccional, por periodos de tiempo, por Sebek, etc. Un ejemplo podría ser, consultar por las conexiones TCP bidireccionales iniciadas desde la Honeynet.

La sección de Detalle muestra en detalle las conexiones, estando ordenadas desde la más antigua en la parte superior a la más nueva en la parte inferior. En el detalle de cada conexión se incluye el tipo de protocolo, el número de bytes del paquete, el tipo de Sistema Operativo y la IP que inició dicha conexión. Si dicha conexión contara con algún alerta de Snort ésta también sería listada en el detalle de la conexión.

A la izquierda de cada conexión aparecerán varios iconos, esto dependerá si los Honeypot cuentan con Sebek instalado o no. Si los Honeypot no cuentan con Sebek instalado sólo aparecerán dos iconos por cada conexión, estos serán un diskette y una lupa. Ahora, si el Honeypot cuenta con Sebek instalado además de estos iconos aparecerán dos iconos más, una flecha azul y un grafico de árbol. Todos ellos serán descritos a continuación.

Diskette: Al realizar un clic sobre este icono, se puede descargar en formato pcap lo datos relativos a ese flujo, o si prefiere puede configurar el navegador para ejecutar alguna herramienta para analizar los datos de pcap, como por ejemplo Ethereal.

Lupa: Al realizar un clic sobre este icono, se podrá analizar la conexión más detalladamente mediante Snort. Esto lo llevará a la Sección de Examen de Flujos, lo cual permitirá analizar con mayor detalle cualquier alerta del IDS, Snort y además realizar la decodificación de los paquetes del flujo

Flecha Azul: Al realizar un clic sobre este icono, se obtienen todas las conexiones relacionadas con este flujo.

Gráfico de Árbol: Al realizar un clic sobre este icono, podrá analizar en detalle todas las actividades del sistema, incluyendo procesos, archivos abiertos, etc. La primera pantalla que aparecerá será la del grafico de árbol de todos los procesos con sus respectivos hijos. Al hacer un clic sobre algún proceso en particular, podrá obtener una mayor información detallada de dicho proceso. Además, si se realiza un clic en la opción que aparece en la parte superior podrá observar los detalles de este proceso, obteniendo un listado detallado de los archivos abiertos y las actividades de lectura realizadas.

Por ello es de suma importancia contar con la interfaz Web funcionando correctamente, ya que mediante esta se puede realizar un análisis acabado de los datos obtenidos por el Honeywall.

4.4 Plan de Pruebas Realizado a la Honeynet

Para validar el Sistema, se realizará una intrusión real. Donde paso a paso se irá observando el comportamiento y reacción del sistema para así verificar claramente cómo responde a este ataque.

Antes de realizar las pruebas se supondrá que la única información conocida es el nombre del dominio de la red el cual es lab1.inf.uach.cl y que el atacante se encuentra en la red del Instituto. Los demás datos serán obtenidos a partir de los distintos métodos y herramientas que se utilizarán para realizar una intrusión en el sistema.

Lo primero en realizar sería la Obtención de la Información y el Análisis de la misma. Para ello se utilizaran herramientas capaces de realizar Who is, Footprinting, Fingerprint y Scanning.

Una vez obtenida la información del equipo o equipos pertenecientes a la red, se dará paso a la siguiente etapa que consiste en enumerar y detectar las vulnerabilidades que estos posean.

La siguiente etapa será ingresar en el sistema y obtener algún tipo de información de los equipos. Para ello, se explotaran las vulnerabilidades, se hará un escalada de privilegios y finalmente se analizaran los resultados obtenidos.

Lo dicho anteriormente se puede resumir en:

1. Obtención y Análisis de Información mediante Who is, Footprinting, Fingerprint y Scanning.
2. Detección y Enumeración de Vulnerabilidades.
3. Explotación de Vulnerabilidades.
4. Ingreso al Sistema.
5. Escalamiento de Privilegios.
6. Obtención de Información Privilegiada.

La idea primordial es lograr una intrusión exitosa verificando la reacción de la Honeynet y cómo esta detecta en todo momento la presencia del intruso. Por ello, en cada una de las etapas que siguen a continuación se podrá observar la intrusión tanto desde el punto de vista del atacante como del administrador del sistema.

4.4.1 Primera Etapa

Lo primero en realizar es comprobar el estado que presenta el Honeywall. Para esto, se debe acceder a la página de administración que se encuentra en https://146.83.216.154/. Como se puede observar en la Figura Nº42, antes de realizar las pruebas se tienen 73 conexiones en total y 28 conexiones bidireccionales.

Figura Nº 42 Honeywall antes de las pruebas

Durante la realización de las pruebas se tendrá las dos visiones la del hacker y la del administrador del sistema. Cómo ya se pudo observar, el sistema tiene un tráfico relativamente normal. Esto, es lo que está viendo el administrador del sistema.

La primera acción por parte del hacker será realizar un ping al dominio ya que es lo único que conoce. En la Figura Nº43 se puede ver claramente esta acción.

```
C:\>ping lab1.inf.uach.cl

Haciendo ping a lab1.inf.uach.cl [146.83.216.152] con 32 bytes de datos:

Respuesta desde 146.83.216.152: bytes=32 tiempo=1ms TTL=64
Respuesta desde 146.83.216.152: bytes=32 tiempo=1ms TTL=64
Respuesta desde 146.83.216.152: bytes=32 tiempo=1ms TTL=64
Respuesta desde 146.83.216.152: bytes=32 tiempo=1ms TTL=64

Estadísticas de ping para 146.83.216.152:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 1ms, Media = 1ms

C:\>
```

Figura Nº 43 Ping realizado por el intruso

Ahora, que el atacante ya sabe la IP del equipo lo más probable es que haga lo mismo para los equipos adyacentes. En las Figuras Nº44 y Nº45 se puede observar esta acción.

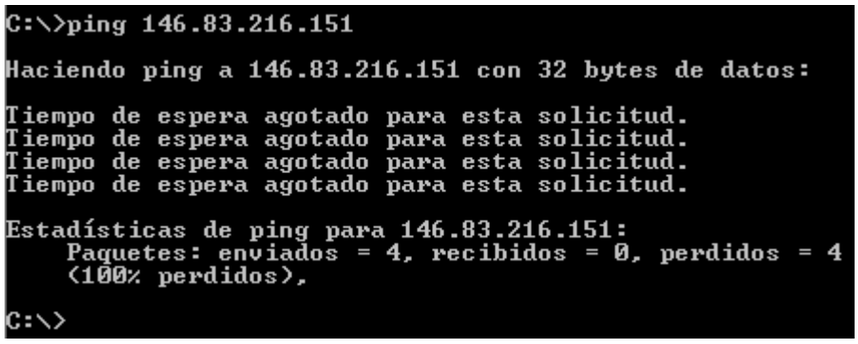


Figura Nº 44 Ping realizado al equipo anterior

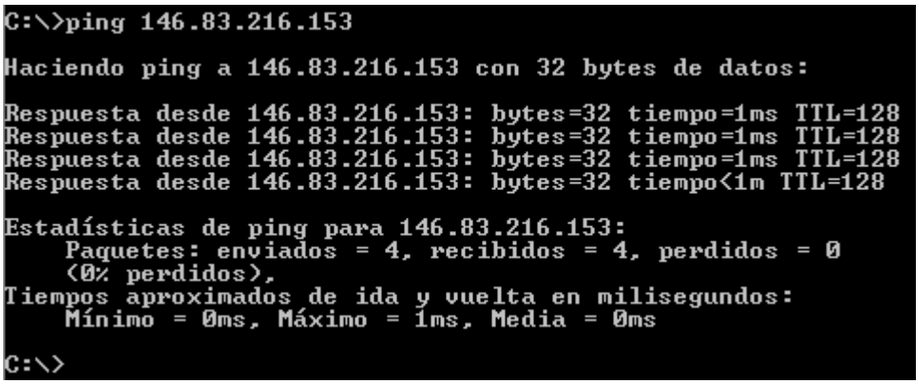


Figura Nº 45 Ping realizado al equipo siguiente

Como se puede ver en las imágenes anteriores esto no le dice nada al atacante, por lo cual lo más probable es que ocupe alguna herramienta que realice ping a una red completa. En esta prueba, sólo se realizó ping a los equipos adyacentes, y el sistema fue capaz de detectar esta acción por parte del atacante. Pero al ojo humano es solamente una conexión más. En la Figura Nº46 se puede ver la respuesta entregada por el sistema.

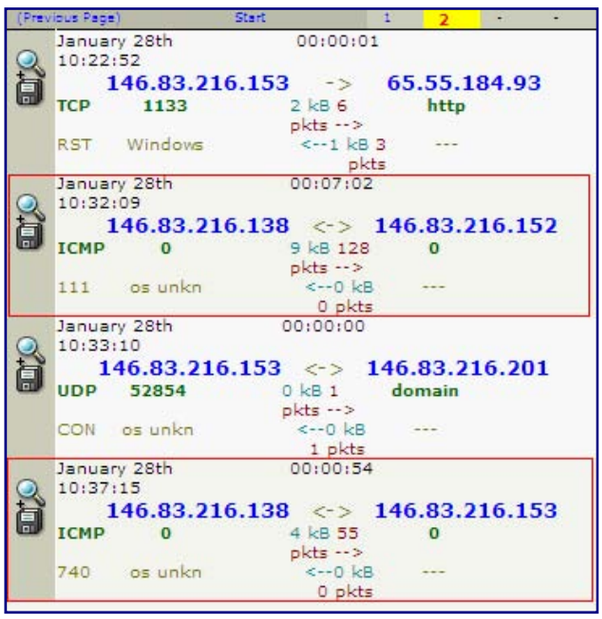


Figura Nº 46 Respuesta del Honeywall a los Ping del Atacante

Lo siguiente que realizará el atacante será obtener una mayor información de los dueños de este dominio. Para ello, se accede a sitios que proporcionan Whois como por ejemplo http://domains.whois.com/domain.php, http://lacnic.net/cgi-bin/lacnic/whois o http://samspade.org/whois/uach.cl. En estos sitios es posible obtener información del dominio, pero no del dominio interno lab1.inf.uach.cl sino que del dominio principal uach.cl. Además, en estos sitios es posible obtener información de las IP como a que empresa está inscrita la IP. En la Figura Nº47 se puede observar las repuestas de estos sitios a las consultas antes descritas.

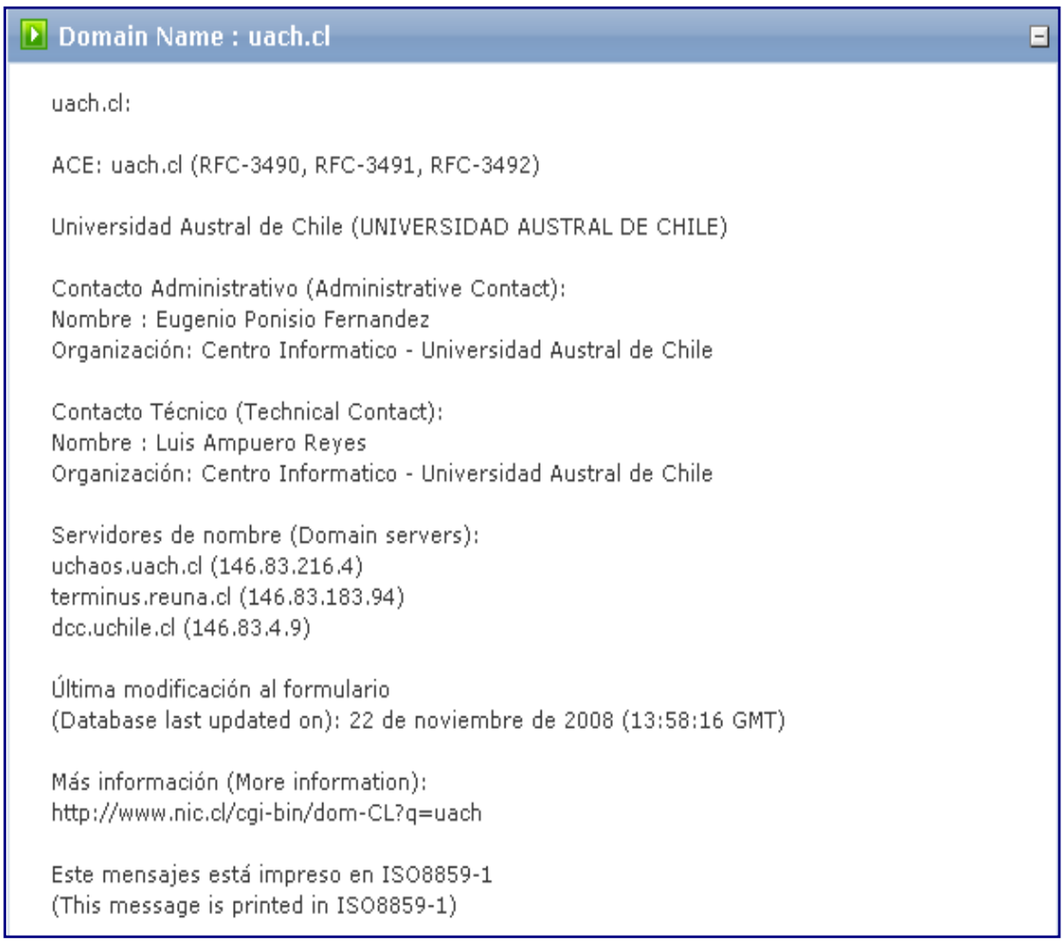


Figura Nº 47 Respuesta del sitio Whois al dominio

En la Figura Nº48, se puede observar las respuestas de estos sitios a la consulta de la IP 146.83.216.152.

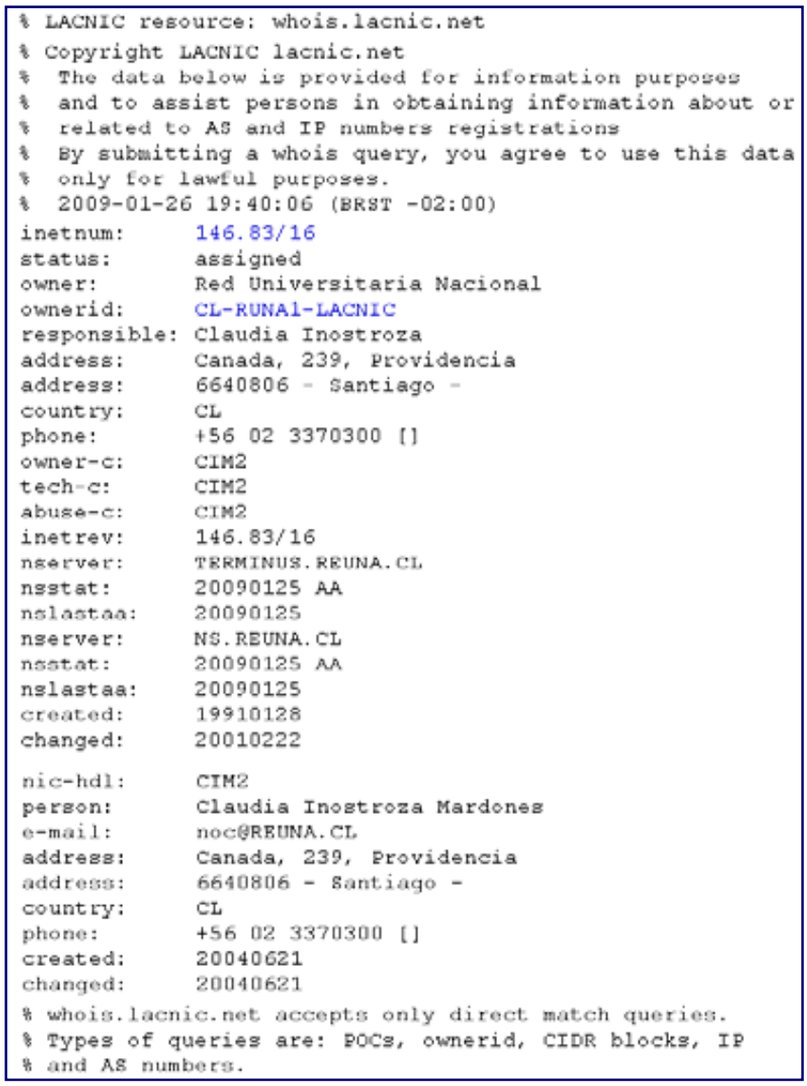


Figura Nº 48 Respuesta del sitio Lacnic a la IP

En las respuestas obtenidas se puede ver como ante la consulta del dominio, las páginas buscan el contenido en www.nic.cl que es la entidad encargada de los dominios .cl y ante la consulta sobre la IP, el contenido es buscado en Lacnic que es el Registro de Direcciones de Internet de Latinoamérica y el Caribe, por ello sólo aparece un *screenshot* alusivo a cada uno. Por esta razón, el Honeywall no entregó ninguna respuesta a la acción realizada por el atacante.

Lo siguiente es ver a qué distancia se encuentra el atacante del servidor, esto se realiza mediante el comando tracert en Windows y traceroute en Linux. En las Figuras Nº49 y Nº50, se puede observar esta acción.

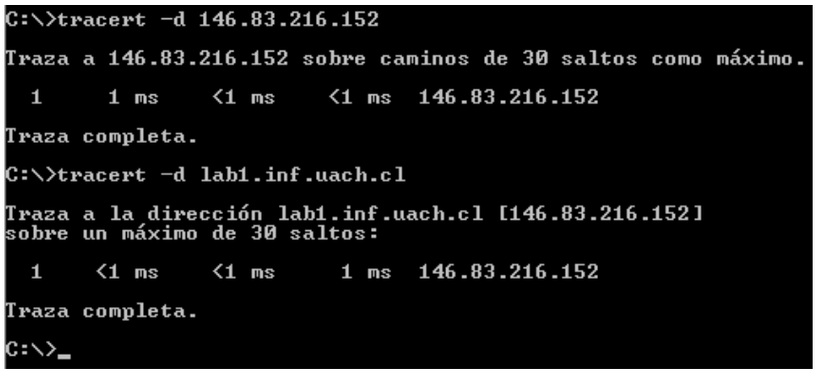


Figura Nº 49 Comando tracert en Windows

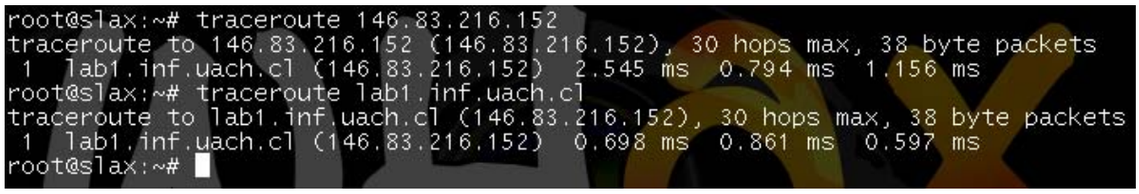


Figura Nº 50 Comando traceroute en Linux

Luego se utiliza el comando nslookup para ver la respuesta del dominio a este comando. Esto se puede apreciar en la Figura Nº51 que sigue a continuación.

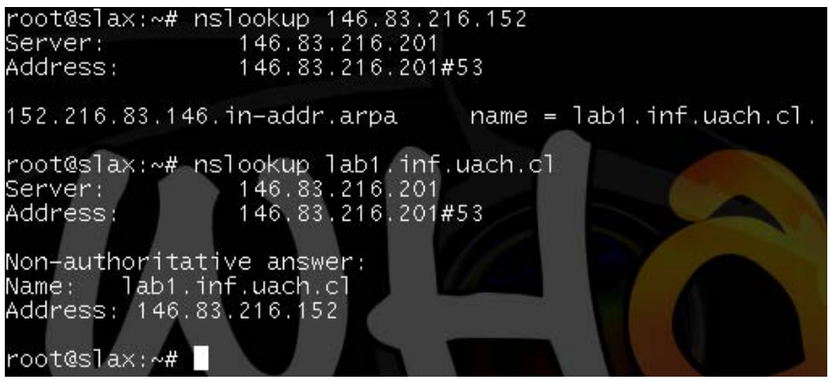


Figura Nº 51 Comando nslookup en Linux

Luego se le da otro uso al comando nslookup, primero asignando como servidor al equipo 146.83.216.152 para comprobar si este equipo es un servidor DNS y ejecutando el comando #ls –d lab1.inf.uach.cl y #ls –d inf.uach.cl. Donde el primer comando no entrega una respuesta positiva, pero el segundo si entrega una respuesta positiva ya que obtiene la zona inf.uach.cl completa. Incluso si se utiliza el comando #ls –d 216.83.146.in-add.arpa se obtiene el archivo de zona inverso.

En la Figura Nº52 se puede apreciar la respuesta del Honeywall ante la ejecución de estas acciones.

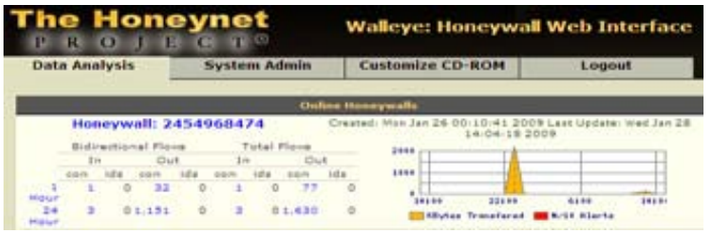


Figura Nº 52 Respuesta Honeywall frente al nslookup

El resultado de todas las acciones anteriores se ve reflejado en sólo cuatro flujos bidireccionales. Por ende es muy difícil para el administrador del sistema poder determinar si está siendo atacado o no. Pero estos pasos realizados por el atacante son sólo una previa para poder obtener información útil por lo cual no logran el fin último del atacante.

El siguiente paso realizado por el atacante es realizar un escaneo de puertos y detección del sistema operativo del servidor, este proceso se denomina Scaning & Fingerprint. Para realizar este procedimiento se utilizará el software Nmap, ya sea en su versión para Linux como para Windows. Nmap para Windows presenta una interfaz de usuario que se denomina Zenmap, la cual permite realizar este proceso de una forma mucho más sencilla.

Además, Nmap permite comprobar el estado de cada puerto encontrado en uno de sus seis estados que son: abierto, cerrado, filtrado, abierto/filtrado, cerrado/filtrado y sin filtrar. Esto permite saber si el equipo se encuentra detrás de un firewall que pueda estar bloqueando los paquetes. En la Figura Nº53 se puede observar claramente la utilización de Nmap en Windows.

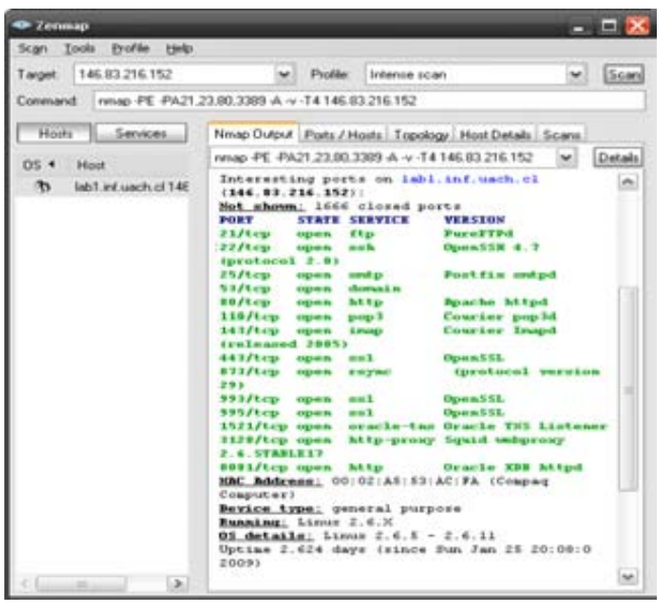


Figura Nº 53 Obtención de puertos y Sistema. Operativo con Zenmap

Como se puede apreciar en la figura anterior mediante Zenmap se pudo obtener los puertos que el equipo tiene abierto así como el sistema operativo que cuenta. Si se cambia de pestaña se puede apreciar más claramente los puertos abiertos como lo muestra la Figura Nº54.

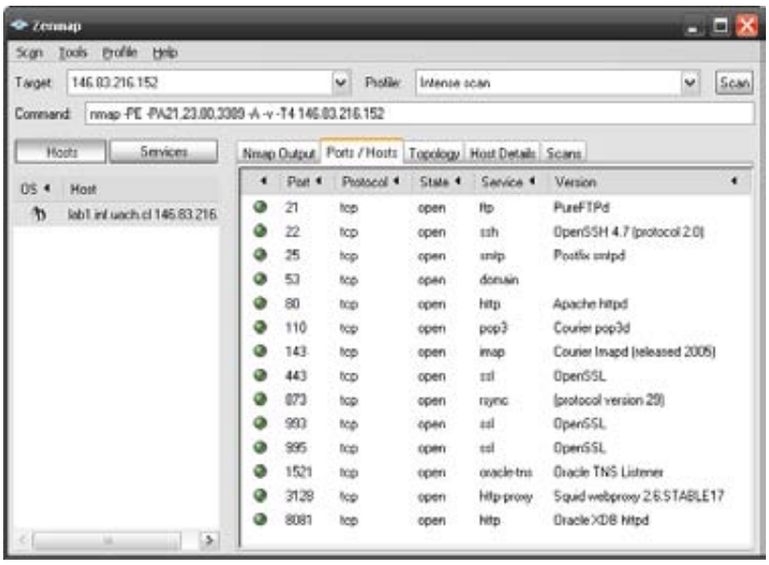


Figura Nº 54 Puertos abiertos del equipo 146.83.216.152 por Zenmap

Luego la pestaña Host Details muestra el Sistema Operativo detectado por Zenmap que posiblemente tiene el servidor en este caso detectó que es un equipo con Linux 2.6.5 - 2.6-11 siendo relativamente efectivo, ya que el equipo cuenta con un Gentoo Linux con kernel 2.6.27. En la Figura Nº55 se puede apreciar lo dicho anteriormente.

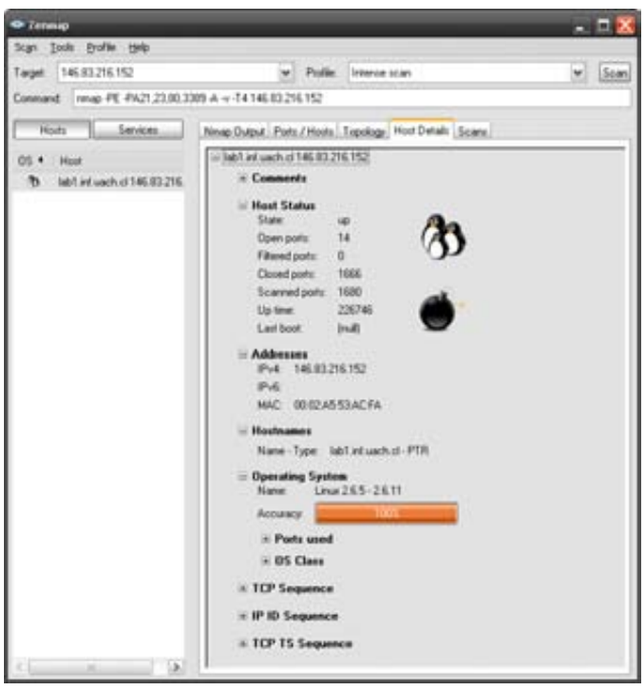


Figura Nº 55 Sistema Operativo detectado por Zenmap

Ante esta acción del atacante, el Sistema responde ya que para obtener los datos se realizan múltiples conexiones lo que indica claramente que alguien está tratando de ingresar al sistema. De 32 conexiones existentes pasan a más de mil conexiones en la última hora esto se puede observar claramente en la Figura Nº56.

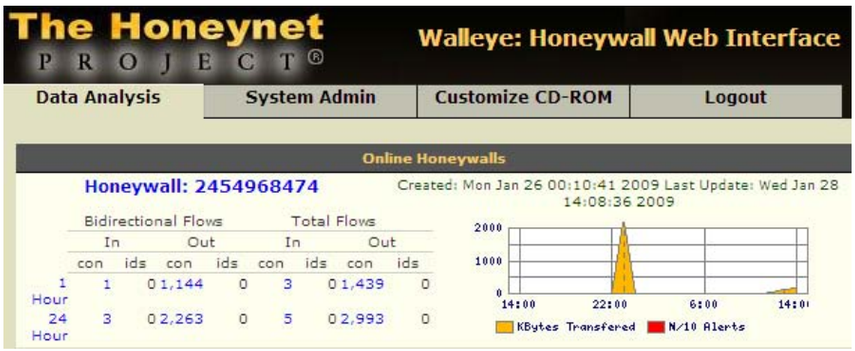


Figura Nº 56 Respuesta del Sistema al uso de Zenmap

Anteriormente se pudo obtener que el equipo 146.83.216.152 fuera posiblemente un servidor de DNS y con el examen de puertos esto queda comprobado al estar el puerto 53 abierto en dicho equipo. Por ello, es conveniente utilizar el comando dig con el cual se puede obtener una mayor información del dominio lab1.inf.uach.cl. En la Figura Nº57 se puede apreciar el uso de este comando y los resultados que entrega.

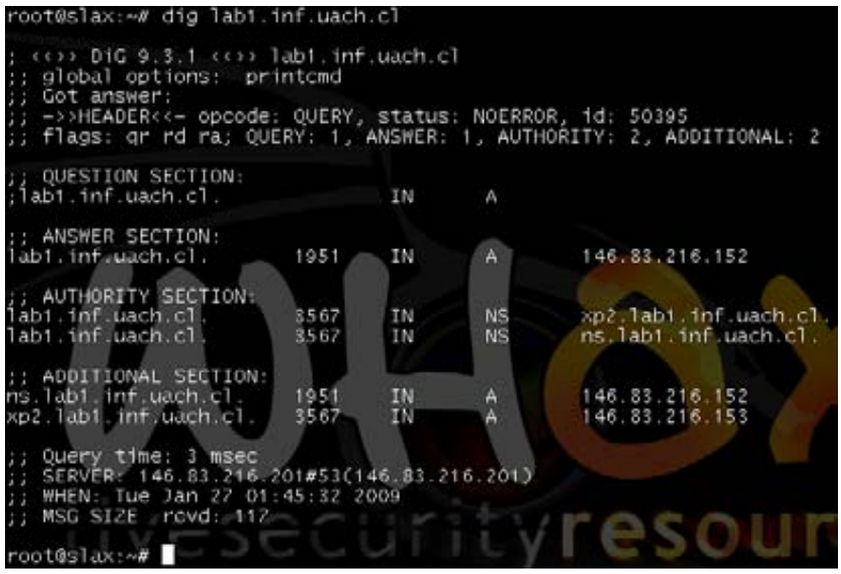


Figura Nº 57 Utilización de dig para obtener información del dominio

Como se pudo observar en la figura anterior no solo el equipo 152 es DNS sino que también el equipo 153, el mismo al que se le había hecho Ping en primera instancia. A continuación en la Figura Nº58, se puede observar un uso más completo del comando dig, donde se puede trazar la ruta desde los servidores principales de Internet hasta el del dominio que se desea consultar.

Figura Nº 58 Información detallada de dig para el dominio

La utilización de este comando sólo produce un leve aumento en 2 conexiones por parte del Honeywall, tal como se puede apreciar en la Figura Nº59.

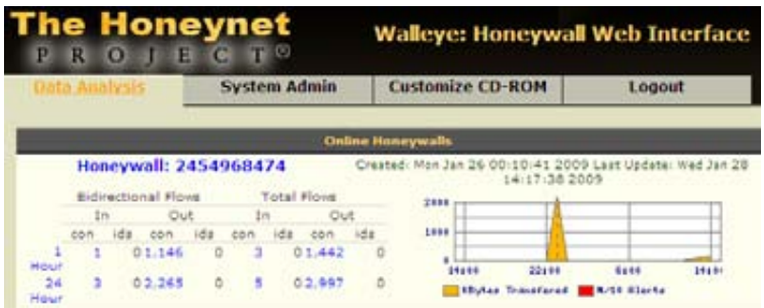


Figura Nº 59 Respuesta del Honeywall ante el comando dig

Mediante el comando anterior se logró descubrir que el equipo 146.83.216.153 también forma parte del dominio lab1 y que además, es servidor DNS de la misma junto al equipo 152. Por ello, es necesario realizar un Nmap a este equipo para obtener mayor información respecto a él. En las Figuras Nº60, Nº61 y Nº62 se puede apreciar el uso de Zenmap en Windows para obtener información del equipo 153.

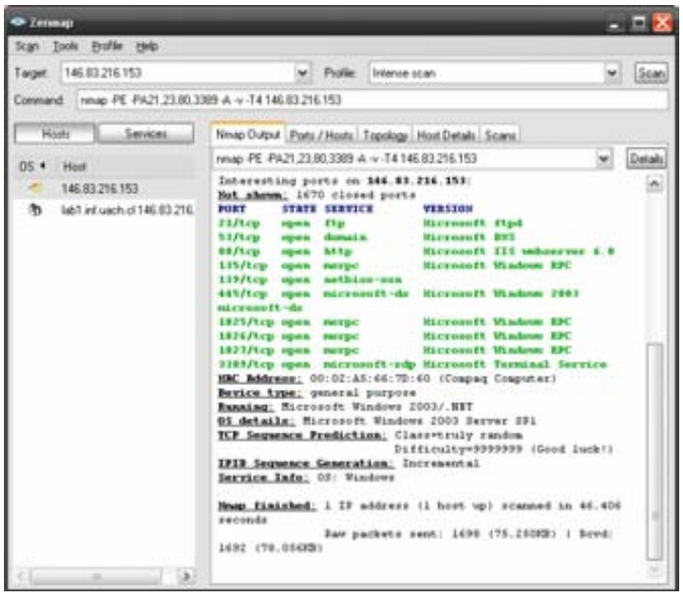


Figura Nº 60 Utilización de Zenmap en el equipo 146.83.216.153

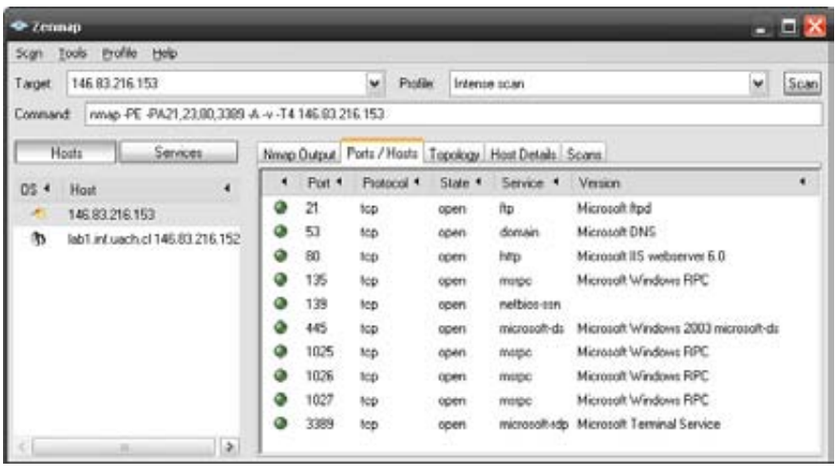


Figura Nº 61 Puertos abiertos detectados por Zenmap

Figura Nº 62 Sistema Operativo detectado por Zenmap

Al igual que con el equipo 152, Zenmap fue bastante acertado con el equipo 153 en cuanto a Sistema Operativo ya que según el software el sistema es Windows 2003 Server SP1 y el sistema operativo que posee el equipo es Windows 2003 Server SP2. Además, dentro de los puertos está presente el puerto 53 que comprueba las sospechas de ser DNS del dominio lab1. El sistema también respondió a la utilización de Zenmap en el equipo 153 como se puede apreciar en la Figura Nº63 que se muestra a continuación.

Figura Nº 63 Respuesta del Honeywall al Zenmap

A continuación en las Figuras Nº64, Nº65, Nº66 y Nº67 se puede ver la utilización de Nmap en Linux, los resultados que arroja y como responde el Honeywall.

Figura Nº 64 Uso Nmap en Linux en el equipo 152

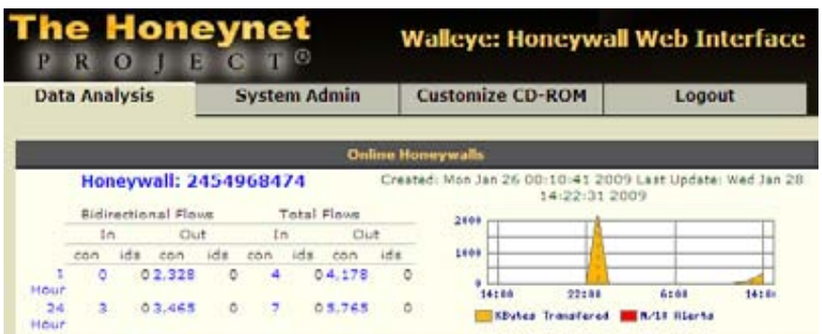


Figura Nº 65 Respuesta del Honeywall al uso de Nmap

Figura Nº 66 Uso Nmap en Linux en el equipo 153

Figura Nº 67 Respuesta del Honeywall al uso de Nmap

En Linux además, se pueden usar otras variantes de Nmap ya que con la opción anterior sólo se obtuvieron los puertos. Estas son –O para obtener el sistema Operativo, -sU para obtener los puertos UDP abiertos y –sO los tipos de ICMP que tiene el equipo. Esto se puede apreciar más claramente en las Figuras Nº68, Nº69, Nº70 y Nº71 que aparecen a continuación.

Figura Nº 68 Detección de Sistema Operativo Nmap del equipo 152

Figura Nº 69 Detección de Sistema Operativo Nmap del equipo 153

Figura Nº 70 Puertos UDP obtenidos por Nmap del equipo 153

Figura Nº 71 Tipos ICMP obtenidos por Nmap del equipo 153

En este caso la detección del sistema operativo para el equipo 152 fue medianamente precisa, pero para el equipo 153 no logró obtener su sistema operativo. Ante estos últimos comandos el equipo Honeywall igual respondió detectando las conexiones realizadas. Esto se puede observar en la Figura Nº72 que aparece a continuación.

Figura Nº 72 Respuesta del Honeywall

Para poder tener más claro qué tipo de sistema operativo cuentan los equipos se utilizará otro software que es xprobe2. Su utilización es relativamente sencilla basta poner xprobe2 –v 146.83.216.152 para obtener el sistema operativo del equipo. A continuación en las Figuras Nº73 y Nº74 se puede apreciar la utilización de este comando.

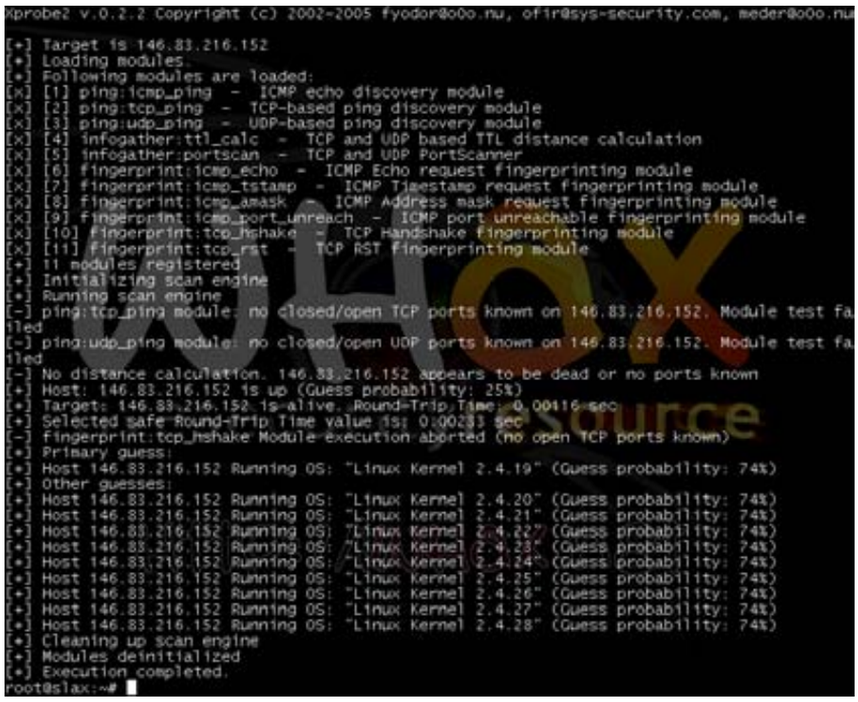


Figura Nº 73 Detección Sistema Operativo de xprobe2 del equipo 152

Figura Nº 74 Detección Sistema Operativo de xprobe2 del equipo 153

Esta herramienta si pudo obtener el Sistema Operativo del equipo 153 y fue relativamente certera, en cambio con el equipo 152 no fue tan precisa. Por ello, el atacante utilizará distintas herramientas para poder estar seguro a qué tipo de equipo se está enfrentando.

Por lo tanto en esta etapa se ha logrado información vital para pasar a la siguiente, ya que se han obtenido los nombres, IPs, puertos y Sistemas Operativos de los equipos principales del dominio lab1.inf.uach.cl.

4.4.2 Segunda Etapa

La segunda etapa consiste en la detección de las vulnerabilidades que presentan estos equipos. Para ello se utilizaran herramientas que permitan hacer la detección de una forma mucho más rápida y sencilla. La razón es netamente para ahorrar tiempo ya que manualmente habría que revisar servicio por servicio para detectar si existe alguna vulnerabilidad, ya sea por ser un software muy antiguo o por una mala configuración del administrador.

Para ello, se utilizaran dos herramientas en Windows y dos en Linux. En Windows se utilizará GFI LANguard Network Security Scanner 8.0 y Tenable Nessus 3, en tanto en Linux se utilizará la herramienta GFI LANguard Network Scanner v2.0 y Saint Exploit. Los reportes de estos softwares se encuentran en el Anexo C, ahí se podrá observar detalladamente los reportes y las vulnerabilidades que presentan los equipos.

En la Figura Nº75 se puede observar el estado en que se encuentra el Honeywall antes de realizar estas pruebas.

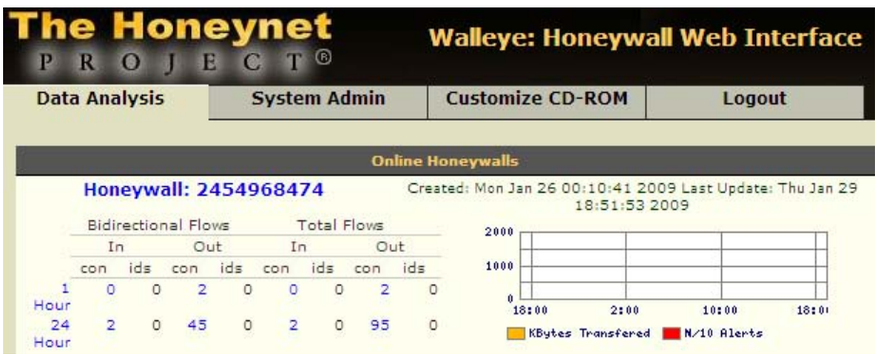


Figura Nº 75 Honeywall antes de los Scanners de Vulnerabilidades

Como se puede apreciar en el Anexo C, tanto el GFI en Linux como en Windows sólo entregaron como vulnerabilidades los puertos abiertos de los equipos y los FTP que permiten a usuarios anónimos.

No ocurre lo mismo con Nessus y Saint, que si detectaron vulnerabilidades e incluso críticas. A continuación se pueden observar más claramente estas vulnerabilidades en la Tabla Nº6.

Tabla Nº 6 Vulnerabilidades de los equipos

Equipo 146.83.216.152	Equipo 146.83.216.153
IBM Lotus Sametime Server Multiplexer Stack Buffer Overflow	IBM Lotus Sametime Server Multiplexer Stack Buffer Overflow
Usable remote proxy on any port - Squid 2.6.STABLE17 is vulnerable	Microsoft Windows Remote Desktop Protocol Server Private Key Disclosure Vulnerability
Vulnerable rsyncd version (protocol = 29)	
Usable remote name server	
Deprecated SSL Protocol Usage	
Weak Supported SSL Ciphers Suites	
DNS AXFR	
HTTP TRACE / TRACK Methods	
Mail relaying	
Proxy accepts gopher:// requests	
OpenSSH 4.7 is vulnerable	
Squid HTTP request smuggling allows cache poisoning	

Las vulnerabilidades de la tabla anterior son la unión de los dos reportes. Las vulnerabilidades en rojo son las consideradas críticas y en naranjo de nivel medio. El Saint Exploit detectó en ambos equipos como vulnerabilidad IBM Lotus Sametime Server Multiplexer Stack Buffer Overflow, aún cuando ninguno de los equipos posee software de la empresa IBM.

Una vez obtenidas las vulnerabilidades lo siguiente es explotar estas vulnerabilidades para así ingresar en los equipos. Esta etapa ha obtenido resultados positivos para el atacante ya que pudo obtener vulnerabilidades importantes en los equipos, como por ejemplo con Squid. Esta vulnerabilidad claramente es una falta de actualización del software junto con una mala configuración por parte del administrador del sistema.

El Honeywall respondió claramente a esta acción del atacante registrando 55.054 conexiones a los servidores como se observa en la Figura Nº76, dándole al administrador del sistema razones más que suficientes para determinar que está siendo atacado y como ya se ha dicho anteriormente al pinchar en estas conexiones puede observar cual es la IP que originó estas conexiones.

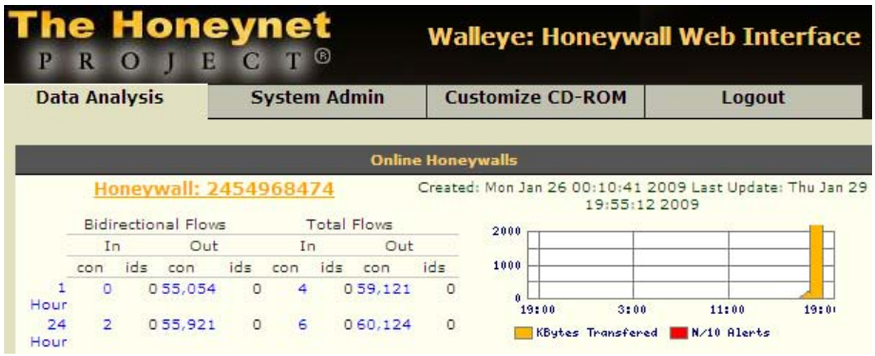


Figura Nº 76 Honeywall después de los Scanners de Vulnerabilidades

4.4.3 Tercera Etapa

La tercera etapa consiste en ingresar a los equipos transgrediendo las vulnerabilidades detectadas en la etapa anterior. Para ello, se utilizará la distribución de Linux llamada BackTrack 3, por ser muy completa y especializada en auditorias de seguridad.

Los softwares que se utilizaran serán Fast-Track y MetaSploit en su versión 3 mediante los cuales se puede realizar una intrusión de forma más sencilla y rápida. Ahora bien, no se explicará en detalle lo realizado en esta etapa por estar fuera del alcance de esta tesis que es ver el funcionamiento de la Honeynet en la red del Instituto y no enseñar hacking a los alumnos del Instituto.

En las dos etapas anteriores se tuvo el IDS desactivado principalmente para ver sólo la cantidad de conexiones producidas por los escáneres. Ahora, en esta etapa se cuenta con el Honeywall funcionando con todos sus servicios. En las Figuras Nº77 y Nº78 se puede observar la respuesta del Honeywall frente al ataque realizado por los meta-exploits. Cabe notar que la cantidad de conexiones es muy superior a las detectadas por el IDS pero esta últimas son las realmente importantes ya que dan a conocer que se está en presencia de un atacante.

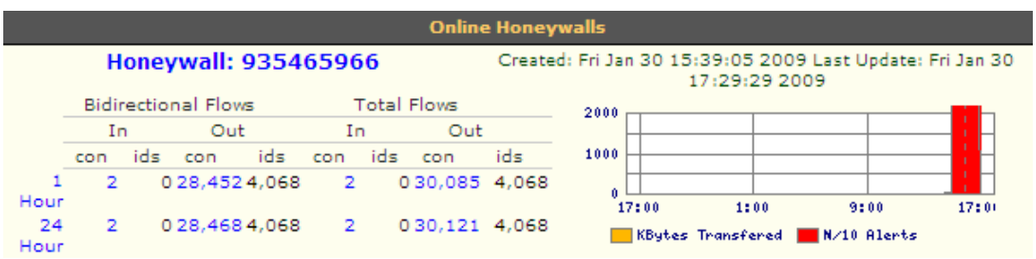
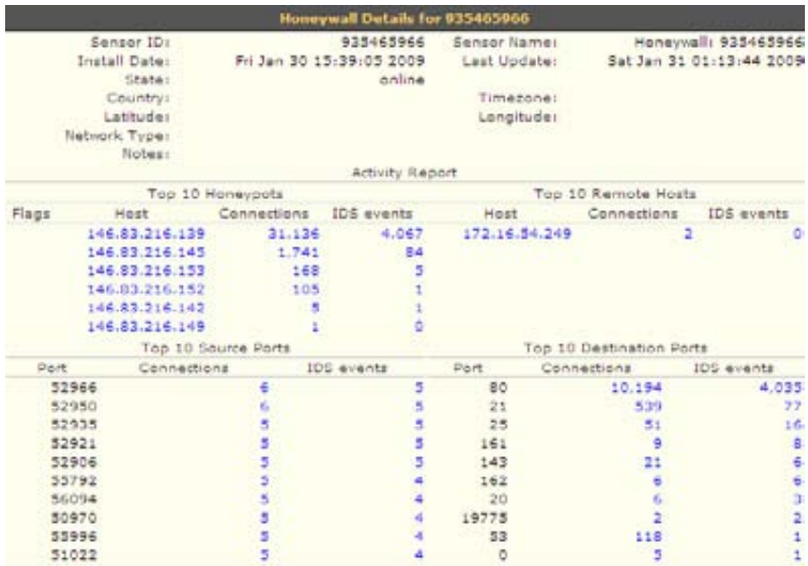


Figura Nº 77 Conexiones detectadas



Honeywall Details for 935465966

Sensor ID:	935465966	Sensor Name:	Honeywall: 935465966
Install Date:	Fri Jan 30 15:39:05 2009	Last Update:	Sat Jan 31 01:13:44 2009
State:	online		
Country:		Timezone:	
Latitude:		Longitude:	
Network Type:			
Notes:			

Activity Report

Top 10 Honeypots

Flags	Host	Connections	IDS events
	146.83.216.139	31,136	4,067
	146.83.216.145	1,741	84
	146.83.216.153	168	5
	146.83.216.152	105	1
	146.83.216.142	5	1
	146.83.216.149	1	0

Top 10 Remote Hosts

Host	Connections	IDS events
172.16.84.249	2	0

Top 10 Source Ports

Port	Connections	IDS events
52966	6	5
52950	6	5
52935	5	5
52921	5	5
52906	5	5
35792	5	4
56094	5	4
50970	5	4
53996	5	4
51022	5	4

Top 10 Destination Ports

Port	Connections	IDS events
80	10,194	4,035
21	539	77
25	51	16
161	9	8
143	21	6
162	6	6
20	6	3
19775	2	2
53	118	1
0	5	1

Figura Nº 78 Equipos que originan las conexiones

Cabe notar también como el Honeywall detecta claramente el origen de cada conexión y a que puerto está destinado. Donde el equipo 146.83.216.139 está generando un gran tráfico de conexiones hacia los Honeypots, donde en gran parte son conexiones malignas.

Al igual que en la etapa anterior el Honeywall detectó todas las conexiones utilizadas por el atacante para ingresar al sistema. Pero, debido a que los equipos tenían sus Sistemas Operativos actualizados, no fue posible ingresar a ninguno de ellos. Por este motivo, el equipo Gentoo fue equipado con una imagen antigua del mismo realizada en enero de 2008 donde tenía el kernel 2.6.19-r5 el cual presenta una vulnerabilidad crítica que mediante un exploit entrega una consola con privilegios de root. Este exploit llamado Linux Kernel Múltiple Prior to 2.6.24.1 Múltiple Memory Access Vulnerabilities[19] afecta a los equipos Linux con kernel inferior al 2.6.24-r1 pero cuya solución es simplemente actualizar el kernel eliminando posibilidad de riesgo.

Al utilizar los programas en la imagen antigua del equipo Gentoo si fue posible tener un acceso a él. Se obtuvo una consola con el usuario nobody y mediante una escalada de privilegios se obtuvo privilegio de root. Esto se realizó de dos formas la primera fue mediante unas ya clásicas instrucciones que se describen a continuación.

```
#cp /bin/sh /tmp/sh

#chown root /tmp/sh

#chmod 4755 /tmp/sh
```

[19] http://www.securityfocus.com/bid/27704

```
#/tmp/sh
```

Con esto se puede obtener una consola como usuario root, la otra forma de hacerlo es utilizar el exploit que aparece en security focus para la vulnerabilidad del kernel. Esto se realiza mediante las siguientes instrucciones.

```
#gcc 27704.c –o exploit

#./exploit
```

Una vez obtenido el acceso como root se accede a los archivos /etc/passwd y /etc/shadow. Como el equipo cuenta con un ftp sólo vasta copiar los archivos o crear un archivo con la salida a pantalla de estos y dejarlos en el ftp para descargarlos.

En las Figuras Nº79 y Nº80 se puede observar los archivos passwd y shadow obtenidos del equipo Gentoo.

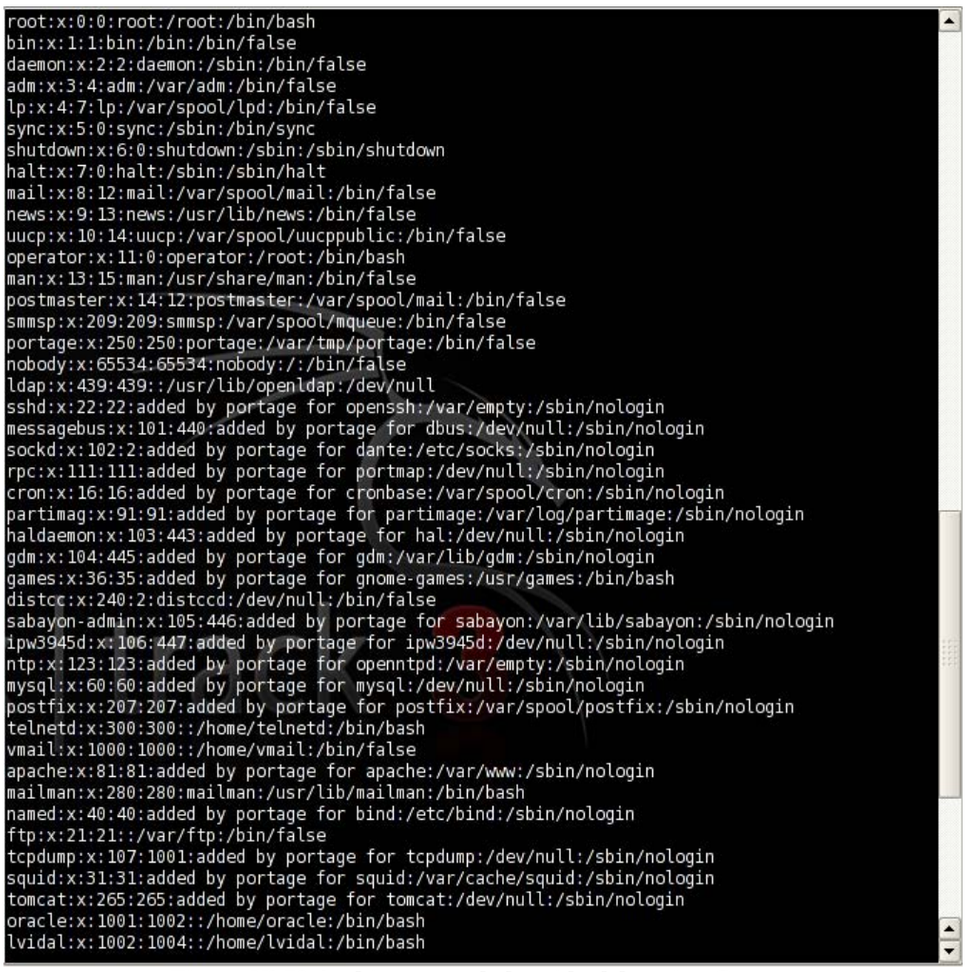


Figura Nº 79 Archivo passwd obtenido del equipo Gentoo

Figura Nº 80 Archivo shadow obtenido del equipo Gentoo

Lo siguiente es mediante un crackeador de password encontrar las passwords de los usuarios del sistema. Como se pudo observar en las imágenes anteriores los usuarios más importantes son root y lvidal, el resto son usuarios del sistema y solo hacen más lenta la detección de las password.

El software a utilizar para obtener las password es LC5 o Lopthcrack versión 5. En la Figura Nº81 se puede observar la interfaz principal del software y como detecta correctamente a los usuarios.

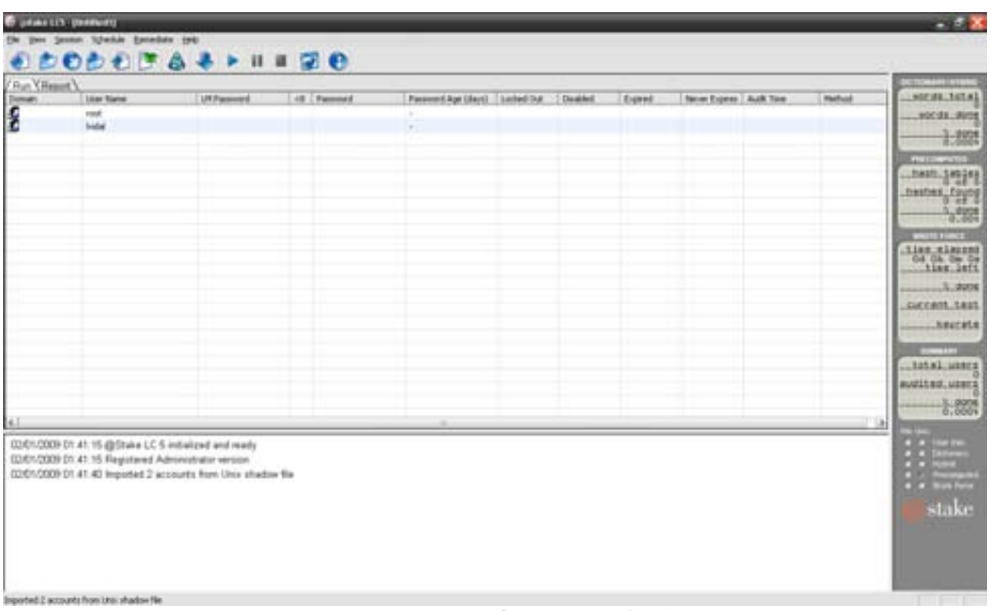


Figura Nº 81 Interfaz principal LC5

Al ejecutar el software encuentra fácilmente el password del usuario lvidal pero para el usuario root va a demorar un tiempo bastante considerable como se puede apreciar en la Figura Nº82.

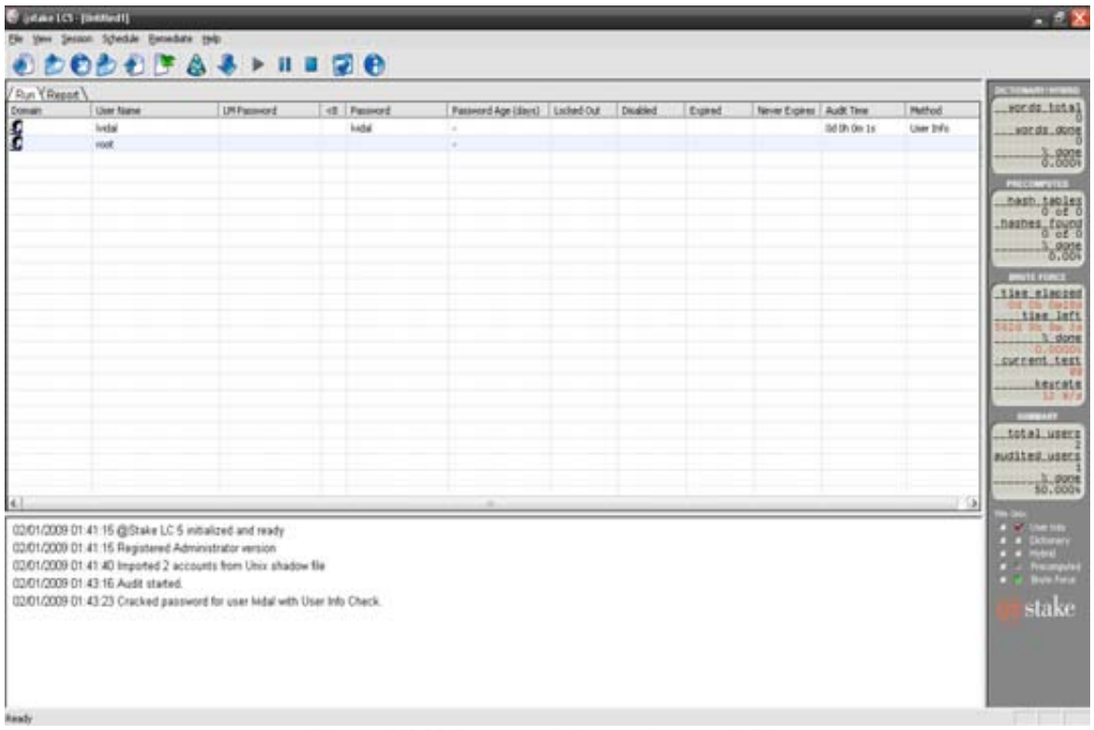


Figura Nº 82 Password detectadas por LC5

Como el tiempo a demorar es demasiado, se prefiere proceder de otra forma. Ingresar con el usuario lvidal mediante SSH, ejecutar el exploit o el /tmp/sh para obtener privilegios de root, para luego editar el archivo passwd modificando el id del usuario de 1002 a 0 al igual que el grupo. Con esto el usuario lvidal pasa a ser administrador del sistema.

Lo siguiente es conectarse de nuevo como lvidal y modificar el password del usuario root mediante el comando passwd root. Con ello, el atacante pasa a ser el dueño del equipo.

Esta última acción, de modificar el password de root, es más para hacer notar el ataque que ha recibido el equipo. Por el contrario, si se quiere mantener un bajo perfil sólo basta con modificar el usuario lvidal o simplemente crear un nuevo usuario con id 0. En la Figura Nº83 se puede observar como se ha tomado posesión del equipo Gentoo.

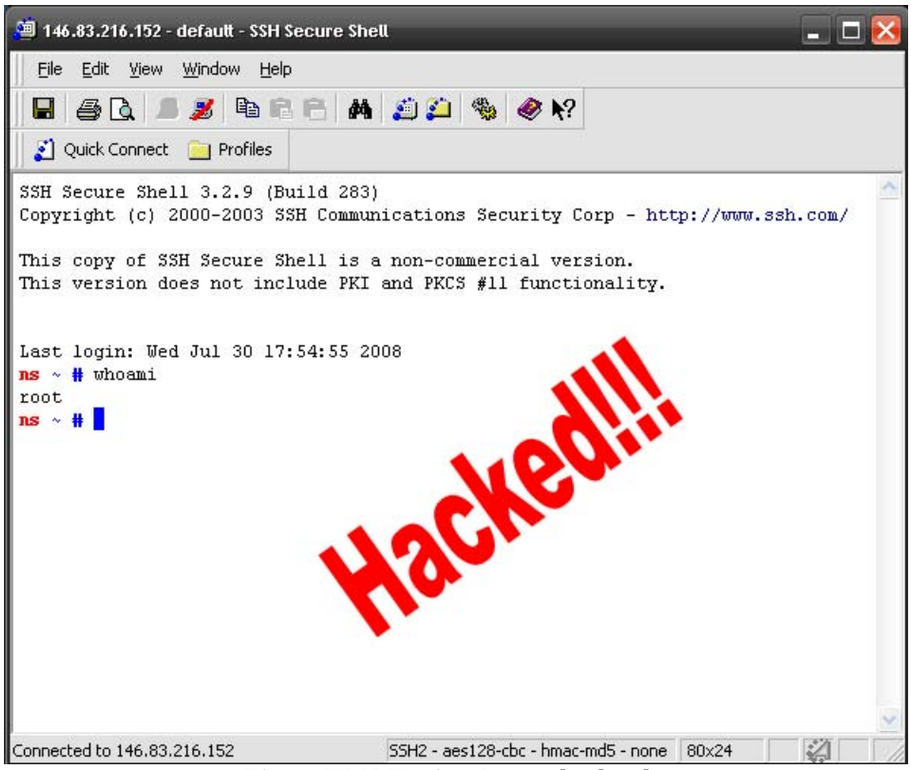


Figura Nº 83 Equipo Gentoo hackeado

Una vez finalizada la detección de password del LC5 no pudo obtener el password de root en un tiempo relativamente corto. Esto se debe a que era una password robusta de 12 caracteres con letras, números y caracteres especiales. La password era *G3nt@@s3rv3r* y no pudo ser detectada por este software que es uno de los más potentes que existen en el mercado. Por ello es indispensable contar siempre con una buena política de passwords.

De las pruebas realizadas al sistema se puede notar la importancia de tener los equipos actualizados y bien configurados para evitar dejar una vulnerabilidad por descuido del sistema. Además, la importancia de tener una buena política de seguridad dentro de la institución, como los accesos a las dependencias, las passwords y sobre todo la seguridad en la red. Por ello, la Honeynet consiste en un medio que permite aumentar la seguridad de la red del Instituto sin afectar el correcto funcionamiento de ésta.

Si los servidores no contaran con el Honeywall el ataque podría haber pasado casi desapercibido. Por ejemplo, si el ataque se hubiera realizado contra el servidor DNS del Instituto que presenta un Linux relativamente antiguo, hubiera sido un éxito para el atacante siendo un blanco relativamente sencillo para él. Por lo tanto la Honeynet permite mantener informado al administrador del sistema sobre los equipos que acceden a los servidores primordiales, si estos acceden indiscriminadamente y maliciosamente evitando que se puedan provocar daños importantes e irreparables en los servidores.

4.5 Resumen

En este capítulo se ha expuesto el desarrollo medular de esta tesis, en la cual se realizó un análisis a la red existente en el Instituto de Informática, exponiendo como es su funcionamiento y como son sus dependencias principales. Posteriormente, se pudo observar la propuesta de Honeynet realizada por el alumno, para un correcto funcionamiento de ésta dentro de la red del Instituto.

Lo siguiente fue dar a conocer como fue implementada la Honeynet, cuáles fueron los equipos, las configuraciones y servicios utilizados. Finalmente, se enseña el plan de pruebas realizado a la Honeynet y cómo responden los servidores principales visto desde las perspectivas tanto del atacante como del administrador del sistema.

Capítulo V CONCLUSIONES Y TRABAJOS FUTUROS

5.1 Resultados Obtenidos

El sistema se encuentra funcionando correctamente en el laboratorio de Tesistas del Instituto de Informática de la Universidad Austral de Chile. Cómo el sistema se diseñó como prototipo, los datos entregados sólo corresponden a las pruebas realizadas con él.

Al evaluar los datos obtenidos por el sistema a nivel cualitativo se pueden apreciar los beneficios que entrega la incorporación de la Honeynet en el Instituto:

- Aumento de la seguridad en la red del Instituto al contar con servidores observados los 365 días del año.
- Permite mejorar el sistema de passwords con el que cuenta el Instituto.
- Mejorar la administración de las IP públicas con las que cuenta el Instituto para así tener un mayor control de los equipos que son ajenos o extraños al uso cotidiano de la red.
- Permite tener informado al administrador del sistema de las nuevas vulnerabilidades y actualizaciones indispensables para los equipos. Lo que conlleva a una mejor administración de estos.
- El sistema se encuentra funcionando con equipos que iban a ser dados de baja por parte del Instituto. Por lo cual, la Honeynet permitió darle un nuevo uso a equipos que no estaban siendo utilizados.
- Es un sistema que se encuentra en el pick de las tecnologías de Seguridad de Informática a nivel nacional, siendo uno de los precursores en este tipo de tecnologías.

Además, el plan de pruebas realizado fue cumplido exitosamente demostrando la validez y viabilidad de la utilización de la Honeynet dentro del Instituto de Informática.

5.2 Conclusiones

La implementación de este prototipo entrega un primer paso para una mejor Seguridad dentro de la red del Instituto. Lo cual, sienta un precedente para ir posicionando al Instituto de Informática a la vanguardia en el campo de Seguridad Informática a nivel Nacional.

El objetivo general de este proyecto de titulo ha sido alcanzado con éxito entregando un prototipo funcional, que permite tener un mayor control de los equipos que son primordiales para la red del Instituto.

La revisión de sitios Web, bibliografía y revistas relacionadas con Seguridad Informática permitió comprender más detalladamente el marco teórico en el que se encuentra inmerso el proyecto, a fin de identificar claramente los distintos tipos de Honeypots, el objetivo que persiguen y sus diferencias. Todo esto se ve plasmado en los capítulos II y III de este documento de Tesis.

El análisis completo de la red del Instituto junto con un diseño acorde a ésta y a los recursos disponibles permitió poner en marcha la Honeynet, siendo ésta, el punto neurálgico de este proyecto. Gracias a esto, se logró un correcto funcionamiento del prototipo implementado, el cual se encuentra funcionando perfectamente en las dependencias del Instituto. Todo lo anterior, se ve claramente reflejado en el capítulo cuatro y el Anexo B de este documento de Tesis.

El plan de pruebas realizado a la Honeynet fue desplegado correctamente y ésta respondió de manera exitosa en todo momento. Las diferencias reflejadas son positivas ya que permite controlar las posibles intrusiones a los servidores principales sin generar un volumen extra de datos.

Las ventajas generadas por la incorporación del prototipo en la red del Instituto tienen que ver con un mayor control y correcta utilización de servidores esenciales dentro de la red. Contar con un mejor manejo de los equipos, una mejor mantención y administración de éstos. Esto permite estar mucho más preparados frente a posibles nuevos ataques que se puedan producir.

El impacto que implica este prototipo se puede ver reflejado en un cambio de mentalidad respecto a Seguridad Informática, ya que permite ver desde un punto de vista mucho más pro-activo. Esto, mejora la Seguridad del Instituto ya no que no sólo se reacciona a los acontecimientos sino que se predicen ataques y se mejoran las políticas de Seguridad.

Si bien este proyecto de tesis fue diseñado como prototipo fue posible obtener conclusiones realmente importantes en cuanto a Seguridad Informática que permiten dar a conocer a los alumnos del Instituto las nuevas tecnologías que se están utilizando en esta materia a nivel mundial, sentando un precedente para la realización de otros proyectos de investigación en este campo de la Informática, que es y será una parte fundamental en cualquier organización.

5.3 Trabajos Futuros

La principal mejora es implementar Sebek en los Honeypots para poder analizar más profundamente los datos del intruso que intenta vulnerar los servidores. Su implementación es relativamente sencilla en equipos comunes pero no funciona correctamente en equipos servidores por ello su implementación en equipos de este tipo sería de gran importancia para el proyecto.

Una posible mejora sería integrar la red inalámbrica del Instituto a la Honeynet para así obtener datos importantes de las personas y equipos que se conectan a la red inalámbrica del Instituto.

La otra mejora sería integrar la Honeynet del Instituto con el proyecto Honeynet a nivel mundial y ser parte de la Organización para así, posicionar al Instituto a nivel mundial en Seguridad Informática.

Capítulo VI REFERENCIAS BIBLIOGRÁFICAS

[ALD98] **Aldegani Gustavo** Seguridad Informática [Libro]. - [s.l.] : MP Ediciones, 1998.

[ANO01] **Anónimo** Linux Máxima Seguridad [Libro] / trad. Arroyo José. - [s.l.] : Prentice Hall, 2001.

[ANO03] **Anonymous** Maximum Linux Security [Libro]. - [s.l.] : Sams Publishing, 2003. - Cuarta Edición.

[AYC06] **Aycock John** Computer Viruses and Malware [Libro]. - [s.l.] : Springer, 2006.

[BEA07] **Beaver Kevin** Hacking for Dummies [Libro]. - [s.l.] : Wiley Publishing, 2007. - Segunda Edición.

[CER08] **CERT** [En línea]. - Agosto de 2008. - 25 de Agosto de 2008. - http://www.cert.org/stats/cert_stats.html.

[CHE90] **Cheswick Bill** An Evening with Berferd [Libro]. - [s.l.] : AT&T Bell Laboratories, 1990. - http://all.net/books/berferd/berferd.html.

[COL05] **Cole Eric, Krutz Ronald y Conley James** Network Security Bible [Libro]. - [s.l.] : Wiley Publishing, 2005.

[DHA03] **Dhanjani Nitesh** Hack Notes - Linux and Unix Security Portable Reference [Libro]. - [s.l.] : McGraw Hill, 2003.

[DOR06] **Dornseif Maximillian [y otros]** Design and Implementation of the Honey-DVD [Conferencia] // Workshop on Information Assurance. - 2006.

[FER08] **Fernández Rafael** Glosario básico inglés-español para usuarios de Internet [En línea]. - 2008. - 25 de Agosto de 2008. - http://www.ati.es/novatica/glosario/glosario_internet.html.

[GAL] **Gallego Eduardo y López de Vergara Jorge** Honeynets: Aprendiendo del Atacante [Informe] / Departamento de Ingeniería de Sistemas Telemáticos ; Universidad Politécnica de Madrid. - Madrid : [s.n.].

[GAR91] **Garfinkel S. y Spafford G.** Practical Unix Security [Libro]. - [s.l.] : O'Reilly, 1991.

[GEN05] **Gentoo** Gentoo Handbook 2005.1 [En línea]. - 2005. - 25 de Agosto de 2008. - http://www.gentoo.org/doc/es/handbook/2005.1/handbook-x86.xml?style=printable&full=1.

[GEN08a] **Gentoo** Gentoo Handbook 2008.0 [En línea]. - 2008. - 25 de Agosto de 2008. - http://www.gentoo.org/doc/es/handbook/handbook-x86.xml?style=printable&full=1.

[GEN08b] **Gentoo** Gentoo Hanbook 2008.0 Trabajando con el Portage [En línea]. - 2008. - 25 de Agosto de 2008. - http://www.gentoo.org/doc/es/handbook/handbook-x86.xml?style=printable&full=1#book_part3 .

[GRA07] **Graves Kimberly** Official Certified Ethical Hacker Review Guide [Libro]. - [s.l.] : Wiley Publishing, 2007.

[GRE06] **Gregg Michael [y otros]** Hack the Stack - using Snort and Ethereal to master the 8 layers of an insecure network [Libro]. - [s.l.] : Syngress Publishing, 2006.

[GRI05] **Grimes Roger** Honeypots for Windows [Libro]. - [s.l.] : Apress, 2005.

[HAT01] **Hatch Brian, Lee James y Kurtz George** Hacking Linux Exposed: Linux Security Secrets & Solutions [Libro]. - [s.l.] : McGraw Hill, 2001.

[HER] **Hernández Miguel José y Lerma Carlos Francisco** Aplicaciones Prácticas de los Honeypots en la Protección y Monitoreo de Redes de Información [Conferencia]. - http://www.honeynet.org.mx/es/data/files/Papers/UAT_Honeypots_ES.pdf.

[HOR03] **Horton Mike y Mugge Clinton** Hack Notes - Network Security Portable Reference [Libro]. - [s.l.] : McGraw Hill, 2003.

[INT08] **Internet World Stats** [En línea]. - 30 de Junio de 2008. - 25 de Agosto de 2008. - http://www.internetworldstats.com/stats.htm.

[ISC08] **ISC ORG** [En línea]. - 30 de Julio de 2008. - 25 de Agosto de 2008. - https://www.isc.org/solutions/survey.

[KUE01] **Kuehl Kirby** The Honeynet Project: Advancements in Honeypot tools [Libro]. - 2001.

[KUE02] **Kuehl Kirby** Intrusion Deception [Libro]. - [s.l.] : Networld+Interop'02, 2002. - http://winfingerprint.sourceforge.net/presentations/.

[KUM95] **Kumar Sandeep** Classification and Detection of Computer Intrusions [Informe] : PhD Thesis / Purdue University. - 1995.

[LEV03] **Levine John** The use of Honeynets to detect exploited systems across large enterprise networks [Conferencia] // IEE Workshop on Information Assurance. - 2003. - http://www.tracking-hackers.com/papers/gatech-honeynet.pdf.

[LON08] **Long Johnny** Google Hacking - For Penetration Testers [Libro]. - [s.l.] : Syngress Publishing, 2008. - Vol. II.

[LUD95] **Ludwig Mark** The Giant Black Book of Computer Viruses [Libro]. - [s.l.] : American Eagle Publications, 1995.

[MAN] **Manunta Giovanni** Seguridad: Una Introducción [Publicación periódica] // Revista Virtual Seguridad Corporativa. - Profesor de Seguridad de Cranfield University http://www.belt.es/bibliografia/HOME2_articulo.asp?id=130.

[MCC01] **McClure Stuart, Scambray Joel y Kurtz George** Hacking Exposed: Network Security Secrets & Solutions [Libro]. - [s.l.] : McGraw Hill, 2001. - Tercera Edición.

[MCM01] **McMullen John** Enhance Intrusion Detection with a Honeypot [Libro]. - [s.l.] : TechRepublic, 2001.

[MCN08] **McNab Chris** Network Security Assessment - Know your Network [Libro]. - [s.l.] : O'Reilly, 2008. - Segunda Edición.

[MIG05] **Migga Kizza Joseph** Computer Network Security [Libro]. - [s.l.] : Springer, 2005.

[MIT02] **Mitnick Kevin y Simon William** The Art Of Deception - Controlling the Human Element of Security [Libro]. - [s.l.] : Wiley Publishing, 2002.

[MIT05] **Mitnick Kevin y Simon William** The Art Of Intrusion - The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers [Libro]. - [s.l.] : Wiley Publishing, 2005.

[ODE03] **O'dea Michael** Hack Notes - Windows Security Portable Reference [Libro]. - [s.l.] : McGraw Hill, 2003.

[OPP06] **Oppleman Victor** Network Defense [Publicación periódica] // Hakin9. - [s.l.] : HardCore IT Security Magazine, 2006. - 17. - págs. 14-25.

[PFL97] **Pfleeger Charles** Security in Computing [Libro]. - [s.l.] : Prentice Hall, 1997.

[PIO05] **Piotrowski Michal** Honeypots - trampa para gusanos [Publicación periódica] // Hacking9. - [s.l.] : Hard Core IT Security Magazine, 2005. - 10. - págs. 48-58.

[POU02] **Poulsen Kevin** Wi-Fi Honeypots a new hacker trap [Libro]. - 2002.

[POU03] **Poulsen Kevin** Use a Honeypot, Go to prison? [Libro]. - 2003. - http://www.securityfocus.com/news/4004.

[PRO07] **Provos Niels y Holz Thorsten** Virtual Honeypots: From Botnet Tracking to Intrusion Detection [Libro]. - [s.l.] : Addison Wesley, 2007.

[RAN02] **Ranum Marcus** A whirldwind introduction to Honeypots [Libro]. - 2002. - http://www.certconf.org/presentations/2002/Tracks2002Expert_files/HE-1&2.pdf.

[ROG08] **Rogers Russ [y otros]** Nessus Network Auditing [Libro]. - [s.l.] : Syngress Publishing, 2008. - Segunda Edición.

[SCA01] **Scambray Joel, McClure Stuart y Kurtz George** Hacking Exposed: Network Security Secrets & Solutions [Libro]. - [s.l.] : McGraw Hill, 2001. - Segunda Edición.

[SCA08] **Scambray Joel y McClure Stuart** Hacking Exposed Windows: Windows Security Secrets & Solutions [Libro]. - [s.l.] : McGraw Hill, 2008. - Tercera Edición.

[SCH06] **Schell Bernadette y Martin Clemens** Webster's New World - Hacker Dictionary [Libro]. - [s.l.] : Wiley Publishing, 2006.

[SCH99] **Schwartau Winn** Lying to hackers is okay by me [Libro]. - 1999. - http://www.nwfusion.com/newsletters/sec/0607sec2.html.

[SEC08] **Security Focus** [En línea]. - 2008. - 25 de Agosto de 2008. - http://www.securityfocus.com/news/552.

[SPI02] **Spitzner Lance** Honeypots: Tracking Hackers [Libro]. - [s.l.] : Addison Wesley, 2002.

[SPI03] **Spitzner Lance** Honeypots: Are They Illegal? [Libro]. - 2003. - http://www.securityfocus.com/infocus/1703.

[STO90] **Stoll Cliff** The Cuckoo's egg: tracking a spy through the maze of computer espionage [Libro]. - 1990.

[THE01] **The Honeynet Project** Know your Enemy [Libro]. - [s.l.] : Addison Wesley, 2001. - http://project.honeynet.org/papers/.

[THE03a] **The Honeynet Project** Defining virtual Honeynets [Libro]. - 2003. - http://his.sourceforge.net/honeynet/papers/virtual/.

[THE03b] **The Honeynet Project** Know your Enemy: Honeynets [Libro]. - 2003. - http://project.honeynet.org/papers/.

[THE04a] **The Honeynet Project** Know your Enemy: Honeynets in Universities [Libro]. - 2004. - http://project.honeynet.org/papers/.

[THE04b] **The Honeynet Project** Know your Enemy: Honeywall CDROM [Libro]. - 2004. - http://project.honeynet.org/papers/.

[THE08] **The Honeynet Research Alliance** The Honeynet Research Alliance [En línea]. - 2008. - 25 de Agosto de 2008. - http://www.honeynet.org/alliance/.

[VER03] **Verdejo Gabriel** CAPÍTULO 4 SEGURIDAD EN REDES IP: Honeypots y Honeynets [Informe] : Tesis Doctoral / Departamento de Informática ; Universidad Autónoma de Barcelona. - Bellaterra : [s.n.], 2003.

[VIL02] **Villalón Antonio** Seguridad en Unix y Redes [Libro]. - 2002. - http://www.shutdown.es/unixsec.pdf.