ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA EN SISTEMAS

TEMA:

"IMPLEMENTACIÓN DE UN SISTEMA DE DETECCIÓN Y ANÁLISIS DE INTRUSIONES NO AUTORIZADAS UTILIZANDO HONEYPOTS CASO PRÁCTICO DESITEL – ESPOCH"

TESIS DE GRADO

Previa obtención del título de:

INGENIERO EN SISTEMAS INFORMÁTICOS

PRESENTADO POR:

Diego Fernando Torres García

Paul Santiago Zambrano Núñez

RIOBAMBA – ECUADOR

2011

El más sincero reconocimiento de nuestra parte para las personas que con su vasta experiencia y dedicación supieron orientarnos a lo largo de la carrera dentro de la prestigiosa Escuela Superior Politécnica de Chimborazo. A la Escuela de Ingeniería en Sistemas al personal docente y administrativo encargados de nuestro bienestar intelectual y personal. Al DESITEL por facilitarnos la información necesaria y el apoyo para la implementación de nuestro plan de tesis dentro de sus instalaciones.

El presente trabajo de tesis está dedicado a mi esposa Ana María, mis hijas Nathalia y Daniela, a mi madre y hermanos pero principalmente al ser que guió mi vida hasta el último día de la suya, la persona que con su ejemplo me motiva hasta el día de hoy desde el cielo, mi padre el Dr. Hernán Antonio Torres Riofrío a quien dedico toda mi carrera y mis estudios.

Diego Fernando Torres García.

La presente tesis está dedicada principalmente a mis Padres Telmo y Olguita quienes con su dedicación y cariño han sabido guiar mis pasos. A mis hermanos Juan Carlos y Telmo gracias por apoyarme siempre, a mi familia y amigos que han estado conmigo en todo momento. En especial a Ubita y Piedadcita por todo el apoyo que me brindaron durante todos estos años.

Paul Santiago Zambrano Núñez.

FIRMAS RESPONSABLES

NOMBRE	**FIRMA**	**FECHA**
Ing. Iván Menes **DECANO FACULTAD INFORMÁTICA Y ELECTRÓNICA**	……	……
Ing. Raúl Rosero **DIRECTOR ESCUELA INGENIERÍA EN SISTEMAS**	……	……
Ing. Danny Velazco **DIRECTOR DE TESIS**	……	……
Ing. Danilo Pastor **MIEMBRO DEL TRIBUNAL**	……	……
Tlgo. Carlos Rodríguez **DIRECTOR CENTRO DE DOCUMENTACIÓN**	……	……
NOTA DE LA TESIS:	……	

Nosotros Diego Fernando Torres García y Paul Santiago Zambrano Núñez, somos responsables de las ideas, doctrinas y resultados expuestos en esta Tesis de Grado, y el patrimonio intelectual de la misma pertenece a la Escuela Superior Politécnica de Chimborazo”

FIRMAS:

---	---
Diego Fernando Torres García	Paul Santiago Zambrano Núñez

ÍNDICE DE ABREVIATURAS

IDS	Sistema de detección de intrusos
CPU	Unidad central de procesamiento
FTP	Protocolo de Transferencia de Ficheros
IP	Protocolo de internet
TCP	Protocolo de Control de Transmisión
UDP	Protocolo de Datagrama de Usuario
MAC	Control de acceso a medios
DOS	Sistema operativo de disco
ICMP	Protocolo de Control de Mensajes de Internet
ARP	Protocolo de resolución de direcciones
CERT	Equipo de Respuesta a Incidentes de Seguridad *Informática*
HTTP	Protocolo de transferencia de hipertexto
HTML	Lenguaje de marcado de hipertexto
SO	Sistema operativo
POP3	Post Oficina de Protocolo
IMAP	Protocolo de acceso de mensajes de internet
SSH	Secure Shell
BOF	
SMTP	Protocolo simple de transferencia de correo
DNS	Servidor de nombres de dominios

ÍNDICE GENERAL

INDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO I

1. MARCO REFERENCIAL

1.1. Introducción

En este capítulo se plantea el estudio y análisis de las herramientas honeypot dentro del DESITEL, para que sea un complemento de las seguridades ya implementadas en la ESPOCH, fortaleciendo de esta forma la defensa ante amenazas externas o internas que buscaran atacar los datos y servicios dentro de la institución.

Se detalla los lineamientos y directrices que ayudaran a desarrollar el proyecto de una forma eficaz y objetiva para evitar contratiempos y redundancias en las actividades y tareas planificadas para encaminar a la investigación correctamente.

Se definirá las metas principales de este proyecto que se deberán cumplir de acuerdo a una ordenada planificación de recursos como: recursos financieros, recursos humanos, recurso tiempo.

1.2. Problematización

1.2.1. Planteamiento

1.2.1.1. Antecedentes

La situación actual de la ESPOCH que centraliza su red en DESITEL en que para la identificación de intrusiones cuenta con un hardware especial con un sistema integrado de firewall, antivirus e IDS la cual protege en tiempo real, filtra contenidos, VPN, detección y prevención de intrusos y gestor de tráfico, además tiene las funciones de alertas, apagado de routers y equipos en caso de ataques. Este dispositivo tiene la capacidad de bloquear, filtrar y proteger todo el contenido de la red de la ESPOCH, inmediatamente luego de la entrada de la Wan, el precio de este equipo es muy alto y además se complementa con otro equipo con el que no cuenta el DESITEL llamado FortiAnalizer también tiene un precio elevado, el cual complementa la seguridad de la red. El FortiAnalizer analiza el tráfico de la red a partir de los datos de registro (logs) generados por el FortiGate, dando a los administradores una visión global de la red.

Los sistemas de detección de intrusos se han convertido en un componente importante en la caja de herramientas de un buen administrador de seguridad. Algunos aún no lo tienen claro, y piensan que un IDS (Intrusión Detection System) puede ser el remedio que nos lleve a la más absoluta tranquilidad y a una irreal sensación de seguridad, más peligrosa en muchos casos que la inseguridad en sí misma. Un detector de intrusos no es más que una de las medidas de seguridad que necesariamente hay que tomar para proteger una red.

Es por ello que se tiene como objetivo reunir información sobre la actividad del intruso. De esta manera seremos capaces de detectar una vulnerabilidad antes de que sea explotada, además de conocer los riesgos a los cuales nuestros sistemas de producción están expuestos. Una de las ventajas de estos sistemas es que proveen de

la información necesaria para conocer los riesgos con los cuales contamos en la red, además de poner de nuestro lado la capacidad de desarrollar seguridad, siendo esto último un punto crucial en la defensa de toda organización o institución.

1.3. Justificación

1.3.1. Justificación Teórica

Como en la actualidad son más frecuentes los ataques que se reciben a través de la red, las técnicas de seguridad y la protección contra ingresos no autorizados han ido creciendo de la misma manera. Es por eso que los Honeypots son una alternativa a este problema los cuales consisten en activar un servidor y llenarlo de archivos tentadores, haciendo que sea difícil, pero no imposible de penetrarlo y sentarse a esperar que aparezcan los intrusos. Esto da a los hackers un gran espacio para recorrer mientras el administrador de la red observa cada movimiento que hacen con el fin de mejorar sus sistemas de seguridad, realizar planes de contingencia y de esta forma evitar futuros ataques.

La ESPOCH cuenta con una aceptable protección de la red, más ningún equipo es completamente invulnerable a ataques interiores o exteriores, por ello Los Honeypots y Honeynets, junto a los IDS, conforman una herramienta cuando hablamos de seguridad en redes. El Honeypot es un software (programas que simulan uno o más servicios de red diseñados en los puertos de un computador), o conjunto de computadores en una red que actúa y parece como una máquina legítima, pero en realidad está configurado para interactuar con hackers potenciales (cuya intención es atraer a crackers o spammers), a fin de obtener información sobre sus estrategias de ataque. Entre más realista sea la interacción, más tiempo estará ocupado el atacante en máquinas "falsas" y lejos de verdaderos sistemas de producción, simulando ser sistemas vulnerables o débiles a los ataques, para poderlos observar en acción;

usualmente está bien aislada del resto de la red, tiene bitácoras extensas (usualmente al nivel de network layer, en una máquina diferente).

Los Honeypots, son una herramienta de seguridad diseñada para ser sondeada, atacada y comprometida, que tiene la capacidad de detectar y registrar estas acciones (registrar los intentos de acceso a aquellos puertos que utilizan generalmente los atacantes), pueden distraer a los atacantes de las máquinas más importantes del sistema, y advertir rápidamente de un ataque, además de permitir un examen en profundidad de los atacantes, durante y después del ataque al Honeypot.

La solución que se trata de implementar en DESITEL es complementar los sistemas de seguridad mediante un HoneyPot de código libre el cual en caso de que cualquier atacante logre violar la seguridad del FortiGate lo encuentre como el primer y más vulnerable sistema a atacar, quedando dentro logs de registro como pueden ser comandos, scripts, inicios de sesión no autorizados, rootkits, troyanos backdoors, etc. Esta valiosa información servirá para detectar las debilidades de los sistemas y combatir futuros ataques utilizando los datos recopilados por el honeypot sin que en el ataque sean afectados los sistemas reales de la institución.

Es por este motivo se ha decidido realizar esta investigación ya que ayudará a la ESPOCH a evaluar los posibles ataques y vulnerabilidades que tienen sus sistemas.

En la actualidad existen aproximadamente 17 herramientas Honeypots de alta interacción entre comerciales y de código libre, para el siguiente estudio se va a tener en cuenta las tres herramientas OpenSource mejor aplicables al caso.

Se eligió utilizar herramientas OpenSource ya que el gobierno ha adoptado la decisión de trabajar con software libre para instituciones públicas, al trabajar con código abierto

el ahorro es significativo ya que no se pagara excesivos costos en las licencias obteniendo también un software de calidad.

La principal limitación para el desarrollo del Sistema de detección de intrusiones es que los Honeypots solo pueden rastrear y capturar actividades que interactúen directamente con ellos. Los Honeypots no podrán capturar ataques a otros sistemas vecinos, al menos que el atacante o la amenaza interactúe con el Honeypot al mismo tiempo.

1.3.2. Justificación Práctica

Con el siguiente tema de tesis se va a resolver:

- Detección de posibles ataques ya sean externos o internos a través de la red de DESITEL – ESPOCH mediante una máquina señuelo ubicada en la DMZ (zona desmilitarizada) previamente preparada para recibir ataques.
- Análisis de logs pertenecientes a las intrusiones no autorizadas a los sistemas del Honeypot descartando los falsos positivos utilizando herramientas propias del mismo.
- Evaluación de resultados y vulnerabilidades de los sistemas debido a los ataques realizados a los sistemas de la ESPOCH.
- Realizar planes de contingencia para evitar futuros ataques del mismo tipo.

Para realizar lo anteriormente mencionado se propone la implementación de un Honeypot el cual deberá estar ubicado en la DMZ que se encuentra inmediatamente luego del FortiGate para así no afectar a la red LAN de la Politécnica y sus tareas habituales

1.4. Objetivos

1.4.1. Objetivo general

- Realizar la implementación de un sistema de detección y análisis de intrusiones no autorizadas utilizando honeypots y aplicar en DESITEL – ESPOCH.

1.4.2. Objetivos específicos

- Estudiar los aspectos generales de la tecnología de detección de intrusiones no autorizadas existentes en la actualidad para conocer así su funcionamiento dentro de la red de la forma más segura posible y sin afectar a otras instancias de la misma.
- Realizar el estudio comparativo de las principales herramientas de los sistemas Honeypots que permitan implementar una tecnología de detección de intrusiones no autorizadas, para establecer la herramienta más eficiente en la implantación de esta tecnología utilizando OpenSource.
- Implementar un sistema Honeypot que permita realizar la tecnología de detección de intrusiones no autorizadas el cual va a solucionar la deficiencia de un sistema para este tipo de análisis dentro de DESITEL.

1.5. Hipótesis

La implementación de un sistema de detección y análisis de intrusiones no autorizadas mediante Honeypots, permitirá conocer de mejor manera el comportamiento de los intrusos y mejorar la seguridad de la red.

1.6. Métodos y Técnicas

1.6.1. Método de investigación científica

Este proyecto hará uso del método científico porque nos da un conjunto de reglas y lineamientos que regirá el procedimiento para ejecutar esta investigación.

1.6.2. Técnicas

Observación: Utilizaremos herramientas para observar el trafico de la red y comprobar que realmente la información se transmite de forma cifrada.

Lluvia de ideas: La lluvia de ideas será una de las principales técnicas para recolectar la información y para procesarla, por el mismo hecho que esta investigación se realizará en equipo.

Entrevista: Se realizará entrevistas al personal administrativo de la JPTCH para obtener los requerimientos para el desarrollo e implantación del portal web de esta institución.

Pruebas del sistema: Las pruebas que realicemos en el sistema con las diferentes herramientas a comparar nos permitirán obtener información para poder elegir la más optima.

CAPITULO II

2. MARCO TEÓRICO

2.1. Introducción

En el presente capitulo se detallan los conceptos básicos que permitirán un mejor entendimientos de lo que se refiere a la historia y funcionamiento de una herramienta de detección de intrusos, sus diferentes tipos y con detenimiento las funcionalidades de los mismos. Además se estudiarán los diferentes conceptos de seguridad informática, posibles amenazas a sistemas, datos y redes dentro de una organización. Se estudiará también la utilización de estrategias de seguridad y los términos fundamentales para la comprensión de los temas que se tratarán en los siguientes capítulos.

2.2. Fundamentos Generales

La tecnología de detección de intrusiones está basada fundamentalmente en la seguridad informática relacionada con la administración de redes y sistemas, se la define como el conjunto de teorías y técnicas orientadas a proteger a los equipos como a los entornos que constituyen a una red, así como toda la información que viaja por ella además de los servicios que ofrece, esto implica que va a garantizar que

dichos recursos sean empleados solo por los usuarios autorizados en el momento en que estos lo necesiten.

Para un mejor entendimiento en lo que se refiere a los fundamentos generales de la tecnología de detección de intrusiones no autorizadas se iniciará con el estudio de la situación actual de la seguridad. El futuro es impredecible ya que, del mismo modo que evolucionan los sistemas y las redes informáticas, aparecen nuevas amenazas que van haciendo de la seguridad informática una actividad más y más compleja y van motivando el desarrollo de nuevas técnicas y estrategias para la lucha contra estos nuevos desafíos.

Los sistemas de información y los datos almacenados son uno de los recursos más valiosos con los que puede contar cualquier organización. La necesidad imperante del flujo de información y el traslado de recursos de un sitio a otro hace que aparezcan vulnerabilidades que ponen en riesgo la seguridad de la infraestructura de comunicación y toda la información que contienen sus nodos. Proteger la información y los recursos tecnológicos informáticos es una tarea continua y de vital importancia que debe darse en la medida en que avanza la tecnología, ya que las técnicas empleadas por aquellos que usan dichos avances para fines delictivos aumentan y como resultado los atacantes son cada vez más numerosos, mejor organizados y con mejores capacidades. Las amenazas que se pueden presentar provienen tanto de agentes externos como de agentes internos, por eso es importante que toda organización que quiera tener una menor probabilidad de pérdida de recursos por causa de los ataques a los que se expone defina una estrategia de seguridad fundamentada en políticas que estén respaldadas por todos los miembros de la organización.

Se debe considerar que la violación de la seguridad en un sistema podría llegar a afectar gravemente las operaciones más importantes de la empresa y dejarla expuesta a la quiebra.

En este trabajo se discute el tema de seguridad de la información, se destacan mediante ejemplos las características más importantes de los mecanismos que actualmente utilizan los atacantes de la red, se identifican los fundamentos para el desarrollo de un sistema de gestión de seguridad de la información y para la creación de una estrategia de seguridad basada en políticas, se desarrolla un modulo de software para la redacción y almacenamiento de políticas de seguridad de la información y se analizan algunas de las herramientas de gestión de seguridad existentes.

2.3. Seguridad informática

2.3.1. Concepto

La seguridad informática es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta (incluyendo la información contenida). Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

2.3.2. Fundamentos de seguridad informática

Como se mencionó anteriormente es fundamental tener en cuenta la seguridad informática de los sistemas para una organización con el fin de prevenir la aparición de

posibles incidentes, salvaguardar los activos informáticos propios, detectar agresiones o intentos de agresión contra dichos activos, recuperar la actividad normal tras un incidente, aprender de los errores que hicieron posible su aparición y descubrir y, si es preciso, denunciar al responsable del incidente.

La seguridad de una compañía es el resultado de la aplicación de una serie de medidas. Estas medidas pueden clasificarse, dependiendo de la función que tengan por objeto dentro de la seguridad de la empresa, cuanto menos, en uno de los siguientes grupos:

- **Prevención o defensa:** En este punto se va a tratar de aquellas acciones destinadas a minimizar la posibilidad de que se materialice una amenaza sobre un determinado activo de la organización. Su objetivo es la minimización de los riesgos.

- **Salvaguardia:** Es lo que va a agrupar las distintas actividades orientadas a reducir al mínimo el perjuicio producido por un incidente en caso de que las acciones de defensa no consigan evitar su consumación.

- **Detección:** Contiene los mecanismos que tienen por misión revelar atentados o intentos de atentado contra los activos a defender, ya sea mientras se produce el incidente o tras su aparición. Por lo general serán más graves las consecuencias cuanto más tarde se produzca esta detección.

- **Recuperación:** Se trata del conjunto de tareas encargadas de garantizar una rápida recuperación de los daños infringidos por un incidente que no se ha podido sortear.

- **Aprendizaje:** Engloba aquellas actividades dedicadas a la corrección de las medidas de seguridad de la organización en función de las nuevas técnicas que puedan ir apareciendo en el mercado o de la experiencia extraída de los errores cometidos en el pasado.

- **Denuncia:** Está compuesto por las distintas acciones encaminadas a identificar las causas y los causantes de un incidente. Tienen por objetivo la depuración de responsabilidades y, si procede, la denuncia del agresor ante quien proceda.

2.3.3. Ciclo de seguridad

La seguridad es una actividad que trata de proteger un grupo de recursos frente a una serie de posibles amenazas. Esta definición, si bien es bastante generalista, es válida para la seguridad aplicada a cualquier campo y, cómo no, sirve también para la seguridad informática. Para conseguir esta meta es necesario atravesar las cuatro etapas del ciclo de seguridad que muestra a continuación la Figura II.I.

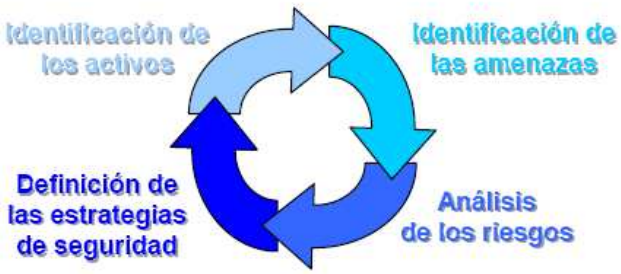

Figura II.I. Etapas del ciclo de seguridad

2.3.3.1. Identificación de activos

Durante esta etapa se localizan y listan los elementos propios que tienen valor para la organización. Estos activos, en el ámbito de la seguridad informática, serán todos aquellos recursos que posea una organización que sea susceptible de ser atacado y cuya pérdida o deterioro de información significaría un daño para la propia organización. Los activos de una compañía podrían clasificarse utilizando las siguientes categorías:

- Recursos físicos.
- Utilización de recursos.
- Software.
- Información almacenada.
- Información en tránsito.
- La imagen y la reputación pública y profesional

Los **recursos físicos** están destinados a su utilización en actividades relacionadas con el desarrollo habitual de la organización. A este uso se refiere el activo identificado como **utilización de los recursos**. Cualquier utilización fuera de la utilidad natural del recurso dentro del contexto de la organización es una amenaza que, de materializarse, puede provocar una reducción de la disponibilidad del recurso o suponer pérdidas económicas para la compañía. Entre las amenazas a la utilización de los recursos se encuentran la utilización del espacio de los discos duros, de los ciclos de reloj de la CPU, del ancho de banda de las redes de la organización.

El software engloba todos los elementos lógicos que hacen uso del hardware y son utilizados en la compañía, como puede ser el sistema operativo, las aplicaciones, etc.

La principal amenaza sobre este activo son los errores humanos y los agujeros de seguridad. Continuamente aparecen nuevas vulnerabilidades que afectan al software informático.

La información es un activo constituido por los archivos y los documentos que son el resultado del trabajo de la organización. Por su naturaleza intangible es almacenada en algún soporte físico y puede ser transmitida a través de las redes de la compañía, lo que la hace vulnerable indirectamente frente a las amenazas a los recursos físicos que se han descrito previamente.

Sin embargo, además de estas amenazas, la información está expuesta a otras nuevas relacionadas con ciertas cualidades que la seguridad informática se ha de esforzar por preservar, tanto cuando la información se encuentra almacenada como cuando está en tránsito:

Disponibilidad: La información ha de ser accesible en el lugar, momento y forma en que sea requerido por un usuario autorizado. Este término aparece muchas veces asociado a la fiabilidad o tasa de fallos. Entre las posibles amenazas a la disponibilidad aparecen los ataques de denegación de servicio contra los servidores de la organización.

Confidencialidad: Sólo las entidades autorizadas deben conocer y tener acceso a la información. No debe confundirse con el término privacidad que se refiere al derecho de una entidad, normalmente de una persona, a mantener su intimidad, a decidir el grado en que desea interaccionar con su entorno, incluyendo el grado de información sobre sí mismo que está dispuesto a compartir con los demás. La confidencialidad es un problema organizacional mientras que la privacidad es un problema individual de cada entidad de la

organización. El espionaje industrial es un ejemplo de ataque contra la confidencialidad de una organización.

Integridad: La información debe ser consistente, fiable y no propensa a alteraciones no deseadas. En este sentido la integridad es la cualidad que garantiza que nadie, que no esté debidamente autorizado, ha hecho modificación alguna en la información almacenada o en tránsito, entendiendo también como modificación la creación o el borrado de la información. Esta cualidad hace precisa la implantación de mecanismos que detecten cambios en los datos. Un ejemplo de atentado contra la integridad de la información podría ser la modificación no autorizada de notas en un sistema escolar, o universitario.

Aparte de estas características, comunes tanto para la información almacenada como en tránsito, hay otras que sólo tienen sentido cuando la información está viajando por la red. En esta situación, las siguientes cualidades habrán de ser igualmente garantizadas:

Autentificación: Es el mecanismo que garantiza que la entidad que accede a un sistema o servicio, ya sea dicha entidad un proceso, un sistema informático o una persona, es quien realmente dice ser.

No repudio: Es el grupo de medidas encaminadas a evitar que el responsable de transmitir una información pueda rechazar la autoría de dicha transmisión. Tiene especial implicación en el correo electrónico para garantizar la autenticidad del remitente.

Protección a la réplica: Esta cualidad garantiza que una transacción sólo puede realizarse una vez, salvo que se especifique lo contrario. Esto sirve para protegerse frente a un ataque que consista en reproducir una llamada a un servicio, capturada previamente, para conseguir la información que obtuvo el usuario autorizado en el momento en que se produjo su llamada original y fue capturada.

La imagen y la reputación pública y profesional es el activo más importante que posee una organización pues puede ser el reflejo de muchos años de trabajo. Un ataque dirigido contra esta imagen o esta reputación puede provocar daños importantes para la empresa que es objeto del ataque, sobre todo cuando se trata de una gran compañía en la que se presupone que se cuida la seguridad, cuando la empresa atacada se dedica al desarrollo de software o de sistemas de red, o más aún cuando el ataque se materializa contra una empresa dedicada directamente a la seguridad informática.

En este tipo de organizaciones un simple ataque, como la modificación del contenido de su página web, aunque no cause daños materiales importantes a priori, puede llegar a ocasionar unas pérdidas astronómicas para la organización motivadas por una pérdida de confianza por parte de sus usuarios. Estos incidentes revelan posibles deficiencias en la política de seguridad de la organización, demostrando:

- Incapacidad de prevenir incidentes.
- Incapacidad de detectar incidentes, ya sea a priori o a posteriori.
- Incapacidad de localizar al infractor.
- Incapacidad de evitar que desde la propia organización se causen daños a terceros, con posible responsabilidad civil e incluso penal para la empresa.

2.3.3.2. Identificación de amenazas

Esta etapa consiste en encontrar todas las posibles fuentes que pudieran llegar dañar alguno de los activos de la compañía. Los recursos físicos, también (hardware), incluyen los equipos informáticos, los sistemas constitutivos de la red (routers, switches, hubs, etc.) y el cableado. Entre las amenazas a estos recursos aparecen las siguientes:

- **Catástrofes naturales:** Incendios, inundaciones, tormentas, terremotos, etc.
- **Fallos eléctricos:** Picos y caídas de tensión, ruido electromagnético, problemas debidos a deterioros en el cableado, etc.
- **Fallos en el hardware:** Los recursos físicos de la organización no están libres de averías. Estos fallos son en muchos casos inevitables y sus efectos sólo se pueden minimizar mediante una correcta política de mantenimiento.
- **Amenazas humanas:** Estos daños pueden ser ocasionados o bien de forma accidental, ya sea por inexperiencia o descuido del personal que trabaja para la organización, o bien de forma malintencionada, ya sea por personal interno o externo a la compañía, como puede ser el robo o el sabotaje.

2.3.3.3. Análisis de riesgos

Esta etapa tiene por objetivo valorar las amenazas sobre los activos, en función de la probabilidad de que se llegaran a materializar y sus posibles consecuencias, para decidir qué riesgos se van a tratar de cubrir.

Como se ha definido anteriormente se entiende por amenaza cualquier elemento que pueda comprometer alguno de los activos de la organización. Podría entenderse que el objetivo de la seguridad informática es garantizar que todos y cada uno de los activos de la organización estén protegidos frente a cualquier tipo de amenaza. Sin

embargo, cada acción enfocada a mitigar un riesgo tiene un precio, lo que implica que la seguridad absoluta presenta un costo infinito.

Un riesgo es una posibilidad de que una determinada amenaza se materialice sobre cierto activo de la organización. Para medir su alcance se utiliza un par de términos adicionales, la vulnerabilidad y el impacto del riesgo:

Vulnerabilidad: la vulnerabilidad de un riesgo es la potencialidad y la probabilidad de que una amenaza llegue a realizarse dañando ciertos recursos. La potencialidad indica si es posible o no que se materialice el riesgo, mientras que la probabilidad es una estimación de la frecuencia con que dicho riesgo puede materializarse.

Se trata, en muchas ocasiones, de una magnitud difícil de calcular. En ocasiones no es posible hacer una cuantificación absoluta y sólo se puede hacer de forma relativa mediante una comparación entre las vulnerabilidades de los distintos activos ante las amenazas que los acechan. Esta comparación permite clasificar los riesgos en función de su vulnerabilidad.

Impacto: El impacto de un riesgo es el conjunto de consecuencias que podrían aparecer en el hipotético caso de que una amenaza llegase a materializarse sobre un determinado activo. Para calcularlo se han de tener en consideración todas las posibles implicaciones de la realización del riesgo: interrupción del servicio, pérdidas económicas, materiales o humanas, responsabilidad jurídica, etc. Esta apreciación de todas las consecuencias que puede implicar la realización de un riesgo puede resultar una tarea muy compleja.

Como se muestra en la tabla II.I indica un ejemplo de posibles incidentes que se pueden presentar en la organización ordenados en función de su alcance, esto se

utiliza como base para el diseño de la política de seguridad de cualquier empresa u organización.

Tabla II.I. Riesgos de una organización

RIESGO	ACTIVO	AMENAZA	VULNERABILIDAD	IMPACTO
1	Servidor Web	Incendio	Muy Baja	$ 7500
2	Servidor Web	Ataque Remoto	Baja	$4000
3	Servidor de Correos	Ataque Remoto	Media	$1200
-------	----------	----------	……	……

A partir de la tabla de riesgos, se puede obtener una idea clara de los posibles incidentes que pueden surgir en una organización. Sin embargo, hay otro método utilizado también para analizar el alcance de los riesgos que la acechan: la gráfica de priorización de incidentes, que se muestra en la Figura II.II. Ambos métodos son válidos para decidir, en función de las características y el alcance de cada incidente, en qué medida y sobre qué riesgos han de actuar las medidas de la seguridad informática de la organización.

Como se observa en la Figura II.2., este método consiste en una gráfica en cuyo eje de abscisas se representan las pérdidas asociadas a un incidente, su impacto, y en cuyo eje de ordenadas se dispone la frecuencia de aparición del incidente, su vulnerabilidad.

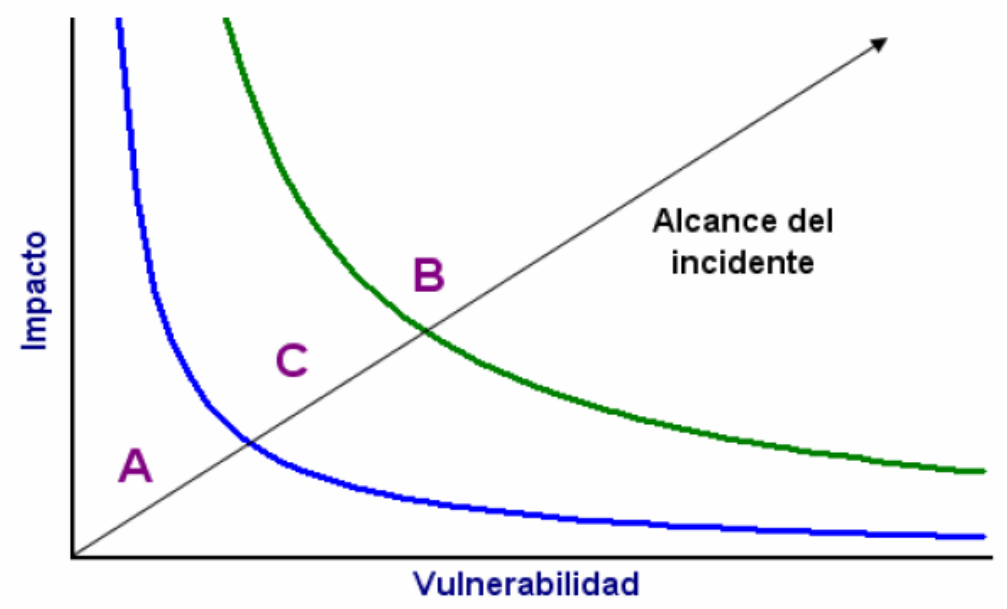

Figura II.2. Priorización de incidentes

Teniendo en cuenta que se ha definido el alcance de un incidente como el producto de su vulnerabilidad por su impacto, se han dibujado sobre la gráfica dos curvas con alcance constante que delimitan tres zonas:

La zona A engloba aquellos incidentes en los que la frecuencia de aparición es muy pequeña o su impacto es demasiado bajo como para ser tenidos en consideración.

Un ejemplo dentro de esta zona podría ser el spam o correo no solicitado. Puede que una organización reciba habitualmente gran cantidad de mensajes de este tipo y que, sin embargo, el daño ocasionado por estos mensajes probablemente sea demasiado bajo para justificar el costo de implantación de las medidas para su filtrado.

En la zona B aparecen los incidentes que, por motivo de su gravedad, la organización no puede en ningún caso tolerar. Se deberán tomar todas las medidas necesarias para mitigar estos riesgos.

La zona C es una zona intermedia en la que los posibles incidentes han de ser tenidos en cuenta a la hora de planificar las políticas de seguridad de la empresa, no engloba riesgos tan insignificantes como los de la zona A, ni tan relevantes como los de la zona B. Para decidir las medidas a tomar en relación con cada incidente que aparezca en esta zona habrá que tener en cuenta otros detalles aparte de su vulnerabilidad e impacto, como puedan ser los recursos económicos, materiales, de tiempo y de personal necesarios para combatir cada incidente.

Estos riesgos aparecen y se extienden, en muchos casos, a una velocidad muy superior a la de las medidas llamadas a solucionarlos. En esta situación no hay modo de reparar la vulnerabilidad y no queda más remedio que afrontar la probabilidad de que la amenaza se materialice. En otras situaciones el costo que supondría mitigar una determinada vulnerabilidad es superior al posible impacto que tendría la materialización de la amenaza. En ese caso es más rentable afrontar el riesgo manteniendo la vulnerabilidad.

Aquí aparece un factor al analizar la zona intermedia de la gráfica de priorización de incidentes. Este factor resultará fundamental a la hora de decidir finalmente qué riesgos se van a cubrir y cuáles se afrontarán sin protección alguna. Se trata del costo de la seguridad. Conseguir un cierto nivel de seguridad conlleva una serie de costos directos e indirectos, entre los que aparecen los siguientes:

Inversiones en equipos y sistemas: Es el costo de los recursos físicos y lógicos utilizados para llevar a cabo las distintas tareas en el ámbito de la seguridad.

Gasto de mantenimiento: Las amenazas son cambiantes. Esta evolución hace que también haya que ir actualizando sistemas y configuraciones para afrontar los riesgos con las garantías necesarias.

Gasto de personal: El costo de los profesionales encargados del desempeño de las tareas relacionadas con la seguridad informática de la organización.

Dificultad de uso: La introducción de nuevas herramientas y aplicaciones puede requerir un cierto periodo de tiempo para que los usuarios asimilen los cambios.

Restricciones de servicios: Para evitar agujeros en la seguridad es necesario que sólo se permita el acceso a los servicios estrictamente necesarios. Esto puede conllevar ciertas incomodidades a los usuarios acostumbrados a utilizar servicios que pueden dejar de estar accesibles.

Reducción de prestaciones: Las medidas de seguridad pueden incluir algún tipo de filtro que a su vez puede ralentizar ciertas operaciones. También es posible que la seguridad introduzca en las redes cierta cantidad de datos adicional que pueda reducir el ancho de banda disponible para el resto de actividades de la organización.

Aparte de estos costos, hay que tener en cuenta también el impacto que tiene sobre una organización el hecho de que una amenaza se materialice sobre un activo determinado, o lo que es lo mismo, el costo derivado de aquellos riesgos no cubiertos por la seguridad informática:

Costos económicos derivados de reemplazar recursos: Es un costo sencillo de calcular que se corresponde con los activos de la organización que se han de reemplazar.

Costos de producción: Se trata de la valoración de lo que la empresa deja de producir durante periodo de tiempo que va desde el instante en que se materializa el riesgo hasta que se restablece completamente la normalidad en la organización.

Costo por negocio perdido: Son las oportunidades de recibir ingresos que pierden las organizaciones durante el periodo de recuperación ante un incidente.

Costos de reputación: Es el costo más difícil de evaluar, pero puede ser muy importante. Este costo se produce por una pérdida de confianza en la empresa por parte de sus clientes.

La seguridad informática es sólo una actividad más dentro de la organización y como tal no puede entenderse de forma aislada a los intereses generales de la empresa, que, por lo general, tratará de maximizar sus beneficios. Dado que la seguridad no produce ingresos, esta intención de maximizar beneficios se traduce en la minimización de los costos.

Para analizar el problema de modo gráfico, como se muestra en la Figura II.3, se utiliza un sistema de coordenadas en el que el eje de abscisas representa el costo para la organización y el eje de ordenadas representa el nivel de seguridad conseguido por la empresa, nivel que va desde el origen, donde la inversión en seguridad es cero y el costo es el costo máximo derivado del impacto de posibles incidentes de seguridad hasta el punto en el que cualquier incidente está previsto y por tanto las pérdidas asociadas a incidentes de seguridad es cero.

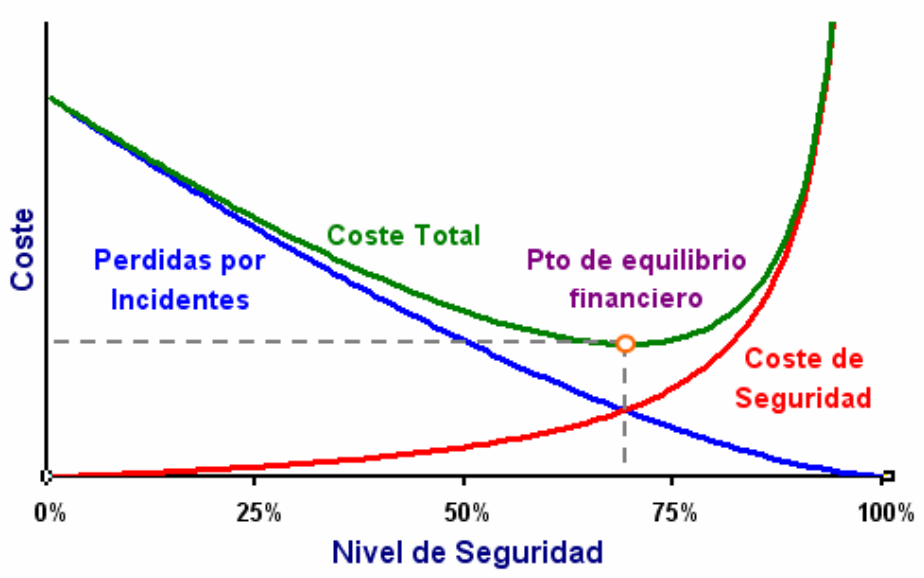

Figura II. 3. Curva de relación costo – nivel de seguridad

Por encima de este punto de equilibrio una mayor inversión con el fin de aumentar el nivel de seguridad de la organización conllevaría un incremento en el costo marginal en seguridad superior al consiguiente decremento en el costo marginal de las pérdidas asociadas a riesgos no cubiertos, mientras que por debajo de este punto aparece el caso contrario.

Este punto define el nivel de equilibrio recomendable, pero es posible que una organización prefiera situarse en un nivel de seguridad superior al definido por el punto de equilibrio. Este podría ser el caso de una empresa de seguridad que utilice como reclamo para ganarse la confianza de sus clientes el hecho de que sus sistemas no hayan sido nunca comprometidos.

Sin embargo, aunque esa situación es posible, el caso más frecuente es el contrario, en el que las empresas, muchas veces inconscientes del alcance de los riesgos, dedican un presupuesto muy pequeño a la seguridad de sus redes y sistemas. En estos casos, si se llega a materializar el riesgo, la empresa puede tener que afrontar pérdidas económicas que pueden ser muy importantes y que de ningún modo han sido previstas.

2.3.3.4. Definición de las estrategias de seguridad

Esta etapa se encarga de tomar todas las medidas necesarias para garantizar que se evitan todos los riesgos que se ha decidido mitigar en la etapa anterior.

2.3.3.5. Desarrollo de las estrategias de seguridad

Como se pudo observar existen varios aspectos que hay que tener en cuenta para la seguridad y estos son: defender, detectar, salvaguardar, recuperar, aprender y denunciar. La finalidad de estas estrategias es el desarrollo de la Política de Seguridad de la empresa, se define como el conjunto de reglas y prácticas que especifican o regulan el modo en que una empresa organiza su seguridad con el fin de proteger sus recursos sensibles. Estas reglas y prácticas, en función de su finalidad, se encuadrarán en una de las siguientes estrategias:

- **Estrategia Proactiva:** Engloba las medidas de prevención, aquellas que se desarrollan para evitar la aparición de incidentes. Tratarán de minimizar el número de puntos débiles del sistema y desarrollar planes de contingencia a seguir en caso de que finalmente se materialice una amenaza.

- **Estrategia de Detección:** Congrega todas las acciones encaminadas a detectar la aparición de incidentes. Implica una adecuada monitorización de cada uno de los recursos a proteger de la organización.

- **Estrategia Reactiva:** Incluye las acciones que se llevan a cabo tras la detección de la materialización de un riesgo. Estas acciones se ocuparán de evaluar el daño asociado a este suceso, conseguir la recuperación de la situación anterior al incidente aplicando los planes de contingencia desarrollados de forma proactiva, documentar el incidente y permitir el aprendizaje a partir de la experiencia.

La Política de Seguridad es un conjunto de requisitos que indican lo que está permitido y lo que no lo está en el seno de una organización. Además, recoge las medidas a tomar en caso de que apareciera algún incidente o cuando alguna de sus normas no fuera debidamente cumplida.

No se trata de una serie de recomendaciones, sino de una lista de normas rígidas de cuyo cumplimiento depende la seguridad de la compañía. Hay una serie de factores que han de quedar suficientemente claros en una Política de Seguridad:

- Alcance de la política, incluyendo los sistemas y las personas sobre las que se aplica.
- Objetivos de la política y descripción de los elementos involucrados en su definición.
- Responsabilidad sobre cada uno de los servicios y recursos implicados en la Política de Seguridad de la organización.
- Responsabilidad de los usuarios con respecto a la información que generan y a la que tienen acceso.
- Requerimientos mínimos para la configuración de la seguridad de los sistemas al alcance de la política
- Definición de las violaciones y consecuencias del no cumplimiento de la política, así como del encargado de imponer y controlar las sanciones por su desobediencia.

Las medidas contempladas en el plan de contingencia tendrán por objeto restaurar el servicio de forma rápida, eficiente, con el menor costo para la organización y causando las menores pérdidas posibles. Para conseguir este objetivo será fundamental un correcto desarrollo de los planes de contingencia de la compañía, que, en la medida de lo posible, no podrá dejar en manos de la improvisación la solución de ningún incidente.

A continuación se muestra un ejemplo de cómo utilizar las directivas para una correcta política de seguridad.

Tabla II.II. Directiva. Intrusiones de personal externo malintencionado

Riesgo	Ingreso en el sistema mediante vulnerabilidades o política de claves ineficiente.
Amenaza	Personal Externo Malintencionado.
Ataque	Intrusión en el sistema.
Estrategia Preactiva	Estimar posibles daños: • Robo y venta de información. • Daño a la imagen de la empresa. Determinar y minimizar las vulnerabilidades: • Actualización de sistemas vulnerables. • Concienciación a los usuarios sobre la utilización de contraseñas fuertes. Evaluar planes de contingencia: • Implementación de servidor de backup para prevenir daños a la información. • Recuperación de la imagen. • Evaluación de métodos para minimizar el daño por la información robada.
Estrategia Reactiva	Evaluar los daños por la información robada y la pérdida de imagen. Determinar el origen de los daños, el punto débil del sistema utilizado. Reparación de los daños. Documentar el incidente. Aprender de lo sucedido. Si procede localizar y denunciar al intruso.
Examinar resultados y eficacia de la directiva	Ajustar la directiva utilizando lo aprendido a consecuencia del incidente.

Las organizaciones verdaderamente concienciadas con los riesgos de la seguridad informática no sólo cuentan con estos medios para realizar las pruebas de las políticas, sino que cuentan con equipos de respuesta a incidentes. Estos equipos

participan en la elaboración de las medidas proactivas y son responsables de actuar ante cualquier incidente o evento inusual que afecte a la seguridad de la compañía.

2.4. Entornos para la utilización de detección de intrusiones no autorizadas

A mediados de la década de los sesenta Marshall McLuhan afirmaba que los adelantos en las telecomunicaciones y la informática convertirían el mundo en una “aldea global”. Internet, nacido como respuesta a la necesidad de compartir información entre ordenadores remotos, se ha empeñado en dar la razón a este visionario y hoy, con más de 650 millones de usuarios repartidos por todo el mundo, se ha convertido ya en la red neuronal de la sociedad actual. Internet ha empequeñecido el mundo. Permite el intercambio de información entre dos máquinas de forma sencilla y eficiente, con independencia de su situación geográfica. Sin embargo, la Red de Redes es insegura por naturaleza.

Se diseñó buscando un modo abierto y flexible de interconexión de redes, pero en la elaboración de sus primeros protocolos no se tuvo en cuenta el tema de la seguridad. Esto explica que en muchos de los servicios que se ofrecen a través de Internet, el intercambio de información se haga en todo momento en claro, sin utilizar criptografía, lo que hace difícil garantizar tanto la confidencialidad como la integridad de la información en tránsito. Esta debilidad afecta a actividades tan habituales como la lectura del correo electrónico, la consulta de páginas web, la transferencia de ficheros mediante FTP o la conexión remota a un terminal mediante TELNET.

Por poner un ejemplo, cualquier individuo que capture los paquetes de una conexión de un cliente con un servidor FTP para la descarga de un fichero, podrá obtener sin ninguna dificultad el nombre introducido por el usuario, la contraseña utilizada para establecer la conexión, las instrucciones introducidas por el usuario y la respuesta del

servidor a cada una de estas instrucciones. Le será posible incluso re ensamblar el fichero descargado por el usuario a partir de los paquetes interceptados.

Aprovechándose de la facilidad con la que cualquiera puede acceder a un equipo remoto conectado a Internet y del diseño inseguro de sus protocolos originales, los ataques a través de La Red son, por lo general, rápidos, sencillos y baratos, a la vez que pueden ser muy difíciles de detectar y rastrear.

Un atacante puede actuar desde cualquier parte del mundo ocultando su procedencia. Incluso, no necesita entrar en un sistema para comprometer la confidencialidad, la integridad o la disponibilidad de su información o sus servicios. Todo esto hace que la seguridad informática sea en la actualidad una continua competición entre los atacantes y los profesionales de la seguridad.

En esta pugna, los atacantes tratan de encontrar nuevas brechas en los sistemas y las aplicaciones a las que tienen acceso a través de Internet y desarrollan utilidades que les permiten entrar en aquellos sistemas informáticos en los que encuentran alguna vulnerabilidad. Mientras tanto, los profesionales de la seguridad tratan de corregir los problemas detectados en los sistemas que protegen y trabajan para evitar que cualquier individuo no autorizado tenga acceso a los recursos que tienen bajo su custodia.

2.5. Inseguridad en Internet

Como se ha dicho anteriormente, Internet no es un lugar seguro. Se ha mencionado como principal causa de esta inseguridad su fundamento en protocolos en cuyo diseño no se tuvo en cuenta la seguridad.

Internet crece de forma muy rápida, cada día aparecen nuevas aplicaciones orientadas a funcionar en red y muchas de estas aplicaciones no son diseñadas, configuradas ni mantenidas de forma segura. En su desarrollo, en multitud de ocasiones, no se pone el suficiente cuidado para que ni se repitan los errores presentes en las aplicaciones anteriores ni se introduzcan nuevas vulnerabilidades.

En el diseño de los sistemas operativos actuales se valora mucho su apariencia y su facilidad de instalación y uso. Muchos permiten incluso que un equipo pueda conectarse a internet directamente tras el proceso de instalación sin obligar al usuario a realizar una configuración adecuada del sistema desde el punto de vista de la seguridad. En multitud de ocasiones, esta configuración la realiza el propio sistema operativo de forma transparente al usuario, dejando puertos abiertos y servicios habilitados que a menudo el propio usuario desconoce y pueden suponer un punto débil del sistema.

Otro detalle a tener en cuenta es que este gran crecimiento de Internet hace necesaria la presencia de administradores con experiencia y conocimientos adecuados. La falta de profesionales calificados, junto con la inconsciencia de algunas empresas, hace que haya gente sin la suficiente experiencia a cargo de la seguridad de muchos sistemas, con el consiguiente riesgo asociado.

Por último, aparte de estos motivos que apuntan hacia los responsables de los protocolos, sistemas y aplicaciones que aparecen en Internet, gran parte del riesgo está asociado a los usuarios finales, que a menudo desconocen de los riesgos que corren desde el momento en que están conectados a Internet.

Muchos piensan que no puede ser objeto de un ataque pues tanto su sistema como la información en él almacenada carecen de valor para cualquier atacante. Otros confían ciegamente en las medidas de seguridad de su sistema operativo o tienen una falsa sensación de seguridad tras tomar ciertas precauciones, a menudo insuficientes, como pueda ser la instalación de un antivirus o unos cortafuegos. No se dan cuenta de que continuamente aparecen nuevos programas y se descubren nuevas vulnerabilidades que hacen que ninguna solución sea efectiva de forma indefinida.

Hoy por hoy, existen páginas dedicadas en Internet, como puede ser Packet Store Security [PacketStorm], desde las que se pueden descargar multitud de herramientas, si bien cualquier buscador puede ser más que suficiente para localizar programas capaces de comprometer la seguridad de un sistema informático. Es tan sencillo encontrar tanto estas herramientas como información detallada sobre su modo de empleo, que cualquier individuo que lo pretenda puede convertirse sin demasiado esfuerzo en una seria amenaza.

Estas utilidades, además, son cada vez más fáciles de manejar. En ocasiones llegan a permitir la automatización completa de un ataque, desde la búsqueda de las víctimas hasta el compromiso final de los sistemas vulnerables. Por otro lado, el uso de estas herramientas está cada vez más extendido y, dado que para la búsqueda de víctimas se pueden escanear redes completas de gran tamaño en no demasiado tiempo y sin apenas esfuerzo, cualquier equipo conectado a Internet es una víctima potencial.

El Computer Security Institute, con la colaboración del FBI de San Francisco, elabora anualmente una encuesta sobre los delitos informáticos en los Estados Unidos, si bien los datos recogidos en dicha encuesta son directamente extrapolables a cualquier organización. En la encuesta del 2002 se recogen las respuestas de 503 encuestados,

principalmente grandes compañías e instituciones del estado. Estas son las conclusiones más destacadas de la encuesta:

El 90% de los encuestados detectó violaciones en su seguridad durante los últimos nueve meses.

El 80% reconoce pérdidas económicas debido a estas violaciones.

2.6. Los atacantes

El primer término que viene a la cabeza de cualquiera al hablar sobre alguna intrusión o sobre alguien que ha realizado un ataque a través de Internet es la palabra Hacker. Si bien no es la intención de este texto juzgar la bondad o la maldad de estos individuos es completamente imposible pasar de puntillas por este tema y evitar deliberadamente la utilización de este término en la redacción de un proyecto que versa sobre la detección y análisis de intrusiones.

En su propia terminología, según aparece en The Jargon File [Jargon 02], se entiende por hacker: “Aquella persona que disfruta explorando los detalles de los sistemas programables y viendo cómo sacar el máximo partido de sus capacidades, en oposición a la mayoría de los usuarios que prefieren aprender sólo lo mínimo necesario. Alguien que programa de manera entusiasta, incluso obsesiva, o que disfruta más programando que teorizando sobre la programación, aquel que es bueno programando rápido. También se refiere a la persona experta en algo o aquella que disfruta de los desafíos intelectuales que supone la superación de limitaciones de forma creativa”.

Otra acepción del término hacker es la de “aquella persona que rompe la seguridad de un sistema”. Esta definición, pese a estar muy extendida, no está bien vista por los propios hackers que prefieren el empleo de términos como crackers o blackhats

(hackers de sombrero negro) para referirse a los individuos representados por esta definición. De aquí en adelante, para evitar polémicas, se utilizarán indistintamente los términos atacante e intruso para identificar a aquella persona que accede sin permiso a un sistema informático a través de Internet.

En el mundo de la Seguridad se distinguen dos tipos de atacante con un perfil bien diferenciado: blackhats y script kiddies, distintos entre sí tanto en el grado de sus conocimientos y experiencia como en las herramientas que utilizan y los motivos que les empuja a introducirse en un sistema ajeno. A lo largo de los próximos apartados se irán detallando las características de cada uno de estos grupos de individuos, así como sus motivos y sus herramientas de trabajo.

2.6.1. Blackhats

Los hackers de sombrero negro deben su nombre a los malos de las películas de vaqueros que siempre aparecían con sombrero negro mientras que los buenos vestían sombrero blanco. Se trata de atacantes experimentados, con profundos conocimientos que utilizan para el desarrollo de acciones ilegítimas, lo que les convierte en el exponente más claro de la imagen que gran parte de la opinión pública tiene sobre el término hacker.

Sin embargo, representan el grupo de atacantes menos numeroso, siendo autores de menos del 25% de las intrusiones que se producen a través de Internet [Symantec 03]. Por contra, son gente entrenada y tienen experiencia en este tipo de actividades lo que les convierte en intrusos muy peligrosos, capaces de atacar sistemas protegidos por importantes medidas de seguridad.

Sus acciones suelen estar motivadas por razones económicas o ideológicas y los blancos de sus ataques son generalmente redes de organizaciones específicas o sistemas que contienen información de alto valor. Estas características de sus blancos hacen que en ocasiones tengan que enfrentarse a grandes desafíos en el terreno de la seguridad. Desarrollan sus ataques de forma sigilosa y una vez que entran en un sistema son capaces de borrar su rastro. Sus acciones son difíciles de detectar y registrar, siendo posible que el administrador de un sistema atacado nunca llegue a ser consciente de que el ataque ha tenido lugar. Cada uno de sus movimientos es planificado previamente de manera detallada, aunque dicha planificación pueda llegar a suponer días, semanas e incluso meses de trabajo. Por lo general cualquiera de sus ataques puede descomponerse en las distintas etapas que se describen en la Tabla II.III.

Tabla II.III. Etapas de un ataque dirigido por un blackhat

A	**Encontrar sistemas accesibles en la red a atacar.**
B	Descubrir los servicios accesibles en los sistemas encontrados.
C	Identificar una vulnerabilidad en alguno de los servicios accesibles, ya sea en el sistema operativo o en una aplicación.
D	Desarrollar una herramienta que, aprovechando la vulnerabilidad descubierta, le permita introducirse en el sistema.
E	Lanzar la herramienta desarrollada y controlar el sistema.
F	Borrar todo el rastro del ataque.
G	Mantener el control del sistema sin levantar sospechas.

Por lo general, estos individuos no utilizan las herramientas ni las técnicas difundidas o localizables en Internet ya que éstas pueden estar lo suficientemente estudiadas como para ser fácilmente identificables, dejando un rastro reconocible tras un ataque. Son capaces de descubrir nuevas vulnerabilidades en sistemas y desarrollar sus propias herramientas, pero no suelen divulgar ni las técnicas ni el código que emplean para evitar que su publicación disminuya su utilidad.

Para ocultar su identidad, en ocasiones, atacan múltiples sistemas que utilizan como saltos intermedios durante sus ataques, para así dificultar su posterior rastreo. Es habitual que, con la finalidad de complicar aún más su localización, estos sistemas intermedios estén emplazados en distintos países, distantes geográficamente, con distintos regimenes jurídicos, distinto idioma y distinta zona horaria.

Si bien los objetivos finales en los ataques de estos intrusos se ha dicho que suelen ser sistemas que albergan información de gran valor, este hecho no implica que cualquier ordenador que no cumpla este requisito esté a salvo. Por ejemplo cualquier ordenador doméstico podría ser una buena elección como salto intermedio o como almacén de herramientas, debido a su limitada capacidad de registro y a la escasa atención que sus usuarios suelen prestar a la información recogida por este tipo de sistemas. Otra opción frecuentemente utilizada por estos intrusos como sistema auxiliar para llevar a cabo sus ataques son los sistemas de los centros académicos. Por lo general estos sistemas son utilizados por multitud de usuarios distintos, están bastantes horas al día conectados a Internet, utilizan direcciones IP fijas y en ocasiones ofrecen anchos de banda elevados. Estas características les confieren un alto valor estratégico.

2.6.2. Script kiddies

Un script es un programa que se ejecuta desde línea de comandos sin necesidad de ser compilado. Así, el término script kiddie podría traducirse como “niño de los scripts”, que es un modo despectivo que utilizan los hackers para referirse a aquellos individuos que entran en sistemas utilizando scripts o programas escritos por otros.

Utilizan herramientas desarrolladas por otros hackers pues se les presupone incapaz de escribir su propio código. De hecho, en muchas ocasiones ni siquiera conocen el funcionamiento de los programas que utilizan. Son intrusos mucho menos sofisticados que los blackhats, pero sus ataques son mucho más frecuentes, siendo los responsables de la mayoría de las pruebas, escaneos y ataques que se sufren en Internet. Cerca del 75% de los ataques que se pueden ver hoy en día en Internet llevan la firma de un intruso perteneciente a este grupo.

Su objetivo es comprometer tantos sistemas como le sea posible, invirtiendo para ello el mínimo esfuerzo y sin preocuparse de saber quién es el propietario de cada uno de los sistemas que atacan y comprometen. Los blancos de sus ataques no suele ser sistemas específicos, como suele ser el caso de un atacante avanzado, y su modus operandi es el que aparece en la Tabla II.IV.

Tabla II.IV. Etapas de un ataque dirigido por un script Kiddie

A	**Encontrar cualquier herramienta que le permita explotar alguna vulnerabilidad.**
B	Escanear tantos sistemas como le sea posible en busca de sistemas que presenten la vulnerabilidad que explota la herramienta que han localizado.
C	Emplear la herramienta para atacar los sistemas vulnerables que ha localizado.
D	Utilizar algún programa que le permita ocultar su presencia en el sistema atacado.

Hace unos años atacar un sistema era una actividad difícil que requería de grandes dosis de conocimientos, tiempo y trabajo. Cada ataque requería ir cumpliendo paso a paso cada una de las etapas que se mostraban en la Tabla anterior. Sin embargo, esta situación ha cambiado radicalmente.

En Internet se ofrecen herramientas que simplifican en gran medida todo el proceso de ataque y con ellas ya no es necesario tener unos grandes conocimientos sobre sistemas operativos ni sobre redes para realizar un ataque. Alguna de estas herramientas llega a ofrecer una interfaz gráfica que permite llevar a cabo un ataque o controlar un sistema sin más complicación que el simple manejo del ratón.

2.6.3. Sus motivos

Los motivos que pueden llevar a una persona a realizar un ataque contra un sistema pueden ser muy variados y dependen en todo caso de cada individuo. Pese a esto, hay ciertos patrones que se repiten una y otra vez: Un ataque puede ser simplemente una pieza más en el desarrollo de otro ataque. Un intruso puede querer un sistema para almacenar documentos o herramientas; puede usarlo como sistema intermedio en sus ataques como un salto más para ocultar su verdadera identidad; o puede servir

para escanear otros sistemas o para participar en nuevos ataques. Es habitual el compromiso masivo de sistemas para lanzar ataques de denegación de servicio distribuido contra servidores importantes.

El objetivo de muchos intrusos es conseguir reconocimiento, ya sea reconocimiento público, descubriendo y documentando una nueva vulnerabilidad o desarrollando una nueva herramienta, o reconocimiento dentro de un grupo de atacantes. En estos grupos la categoría de cada intruso suele ir directamente relacionada con la cantidad y con el alcance de sus hazañas en La Red. Dada la ilegalidad o a legalidad de sus acciones es habitual en estos intrusos el empleo de pseudónimos para esconder su verdadera identidad.

Otros muchos hackers dicen desarrollar esta actividad por simple curiosidad. Para ellos es un entretenimiento, una forma de ver cómo funcionan las cosas y cómo se puede forzar un sistema para conseguir saltar una barrera de seguridad. En ocasiones lo hacen por ego, por la sensación de poder que les da el hecho de ser conscientes de su capacidad para entrar en sistemas sin permiso.

No se pueden olvidar los motivos económicos, muchas veces hay dinero detrás de los ataques que tienen lugar en Internet. Las empresas y los gobiernos contratan a este tipo de individuos para vigilar la actividad de otras compañías y gobiernos o para obtener documentos privados o confidenciales. El hacking es una herramienta importante dentro del espionaje industrial y gubernamental.

Una corriente que está tomando mucha fuerza es la representada por los ataques desarrollados por motivos ideológicos. Muchos intrusos explican sus acciones como una consecuencia lógica de sus convicciones políticas o éticas, de lo que

personalmente consideran justo, convencidos de que el fin justifica los medios. Este tipo de motivación es el desencadenante de movimientos como el hacktivismo y el ciberterrorismo, que aparece cuando las acciones desarrolladas para defender unas ideas se llevan al extremo.

2.6.4. Sus herramientas

Como ya se ha dicho, en la actualidad es muy sencillo encontrar en Internet todo tipo de herramientas utilizables para dirigir un ataque, así como documentación detallada sobre su capacidad y su modo de utilización. Dichas herramientas son desarrolladas por hackers, compañías o profesionales de la seguridad y en ocasiones son inicialmente diseñadas con un propósito bien distinto de aquel para el que finalmente son utilizadas.

Hasta hace unos años las utilidades que un atacante tenía a su disposición eran herramientas especializadas, cada una con un rol diferente de modo que para cada etapa del ataque se utilizaba un programa distinto. Se podían encontrar herramientas especializadas en:

- Crear una lista con las direcciones IP asociadas a sistemas activos. Por ejemplo, mediante un escaneo utilizando mensajes ICMP echo request.
- Escanear los sistemas encontrados en busca de vulnerabilidades. Comprueban si un sistema ofrece un determinado servicio y, de ser así, tratan de reconocer la versión del servicio ofrecido para conocer si es vulnerable.

- Atacar una determinada vulnerabilidad. Estos programas, denominados exploits, contienen un código que se ha diseñado para permitir la intrusión aprovechando una vulnerabilidad conocida.
- Averiguar contraseñas, ya sea utilizando una vulnerabilidad en el sistema de claves o mediante fuerza bruta, es decir, probando insistentemente distintas combinaciones de nombres y contraseñas hasta encontrar una pareja nombre de usuario - contraseña válida.
- Capturar paquetes que atraviesan un segmento de red. Este tipo de herramienta es conocida como sniffer.
- Modificar los registros o logs, y los programas que pudieran delatar su presencia en el sistema.

Hoy, sigue habiendo multitud de herramientas especializadas, ya sean programas nuevos o nuevas versiones de las herramientas antiguas. Sin embargo estas aplicaciones han ido evolucionado, cada vez son más sofisticadas y potentes, pero a la vez son más fáciles de conseguir y más sencillas de manejar.

Cada vez es más común encontrar herramientas más complejas que cubren más de una funcionalidad. Un claro ejemplo es Nessus [Nessus], una aplicación desarrollada para ayudar a los administradores a encontrar vulnerabilidades en sus sistemas. Sin embargo, cuando se utiliza con otras intenciones, esta aplicación puede servir para encontrar equipos accesibles en una red, reconocer el sistema operativo que utilizan y los servicios de red que ofrecen y descubrir gran variedad de vulnerabilidades presentes en los sistemas encontrados, y todo esto desde una sencilla e intuitiva interfaz gráfica.

En este sentido, durante los últimos años han aparecido una serie de herramientas, denominadas auto-rooters, que van un paso mas allá y son capaces de automatizar los ataques, encargándose de toda la secuencia de escaneo, prueba y ataque de los sistemas vulnerables.

Estas herramientas, cada vez más populares, se centran en una determinada vulnerabilidad y presentan un sencillo modo de operación: Escanean de forma aleatoria direcciones IP, en un rango elegido por el atacante, en busca de sistemas con la vulnerabilidad buscada y cada vez que descubren un sistema vulnerable lo atacan de forma automática. Esta búsqueda aleatoria del objetivo convierte a cualquier equipo conectado a Internet que posea alguna de las vulnerabilidades buscadas por este tipo de herramientas en una víctima potencial de este tipo de ataques.

En la práctica total de los casos, las vulnerabilidades explotadas por estas herramientas habrán sido encontradas por algún hacker avanzado o por un profesional de la seguridad distinto del individuo que la utilizará finalmente dichas herramientas.

Estos usuarios no necesitan conocer el funcionamiento interno del programa para lanzar un ataque. Sólo necesitan disponer de la herramienta y ejecutar una serie de comandos que, cuando no aparezcan explicados en archivos de texto que acompañan al propio código de la herramienta, podrán encontrarse seguramente en Internet.

Lo preocupante es que estas herramientas están tan extendidas y su utilización es tan simple que cualquier sistema conectado a Internet, aunque su dirección IP cambie cada cinco minutos, más tarde o más temprano será escaneado y si contiene la vulnerabilidad buscada por el intruso será atacado y comprometido.

Una vez que un intruso consigue entrar en un sistema su siguiente objetivo será conseguir privilegios de administrador, si no los tiene ya, ocultar su rastro para evitar ser descubierto y garantizar un modo de acceso al sistema comprometido sin tener que volver a utilizar la vulnerabilidad. Para ocultar su rastro, un intruso necesita modificar aquellos registros del sistema que puedan mostrar evidencias de lo ocurrido. También debe reemplazar los programas encargados de monitorizar la actividad del sistema por otros que oculten su presencia.

Estas modificaciones en el sistema pueden ser descubiertas por los administradores. Existen aplicaciones que, mediante chequeos de integridad del sistema, son capaces de detectar tanto las modificaciones en los registros como el reemplazo de los binarios que monitorizan el sistema. Para evitar esto, el nuevo objetivo de los intrusos para ocultar su presencia es el propio kernel del sistema.

Una última faceta en la que también se ha observado una evolución en las herramientas a disposición de los atacantes tiene que ver con la criptografía. Hasta hace poco los programas implicados en las intrusiones utilizaban texto en claro tanto para sus comunicaciones con la máquina atacada como para sus ficheros de configuración. Sin embargo, cada vez es más frecuente el uso de criptografía tanto en el acceso al sistema, como en los ficheros de configuración, lo que limita en gran medida la capacidad de monitorización de las organizaciones.

2.7. Tipos de ataque

Existe una gran variedad de tipos de ataque cuyo objetivo puede ser la obtención de información sobre un equipo informático o un usuario, el bloqueo de un servicio o el control de un sistema informático. A continuación se explicará brevemente en qué consisten los ataques más frecuentes que se pueden realizar a través de Internet.

Sondeo

Se trata de un intento de acceso al sistema, puede hacerse para tratar de descubrir cierta información sobre el equipo o como paso previo a un ataque.

Escaneo

Consiste en un conjunto de pruebas, realizadas de forma secuencial y automatizada por una herramienta, que tienen la finalidad de conocer la topología de una red. Puede servir para encontrar una vulnerabilidad en un sistema, en ese caso puede ser la antesala de un ataque.

Compromiso de una cuenta de usuario

Significa el acceso y utilización por parte del atacante de una cuenta del sistema atacado propiedad de un usuario legítimo. En dicho sistema gozará los privilegios que posea el dueño de la cuenta.

Compromiso de una cuenta de administrador

A diferencia de una cuenta de un usuario corriente, la cuenta de administrador tiene acceso ilimitado a los recursos del sistema. En definitiva quien tiene acceso a una cuenta con estos privilegios tiene el control del sistema.

Captura de tráfico

Mediante el uso de programas de captura de tráfico, conocidos como sniffers, el atacante tiene acceso a todos los paquetes que viajan por el segmento de red al que accede el programa. En caso de utilización de protocolos que no cifren los datos en tránsito el atacante puede leer y recuperar la información enviada, entre la que puede haber nombres de usuario y contraseñas.

Denegación de Servicio (Denial of Service, DoS)

Estos ataques tienen la finalidad de bloquear o degradar la disponibilidad de un servicio, impidiendo su uso por los usuarios legítimos. Se consigue haciendo llegar a un elemento de red más tráfico del que puede absorber o consumiendo un recurso limitado del sistema atacado. Hay ocasiones en las que el ataque se lanza de forma sincronizada entre varios equipos, en este caso se habla de ataques de denegación de servicio distribuidos o DDoS (Distributed Denial of Service).

Secuestro de una conexión (session hijacking)

En esta ocasión el atacante asume la identidad de un sistema en una conexión establecida entre dos equipos con la finalidad de recibir información destinada al sistema suplantado o para enviar información manipulada al sistema con el que se conecta. Este ataque aparece en ocasiones acompañado por un ataque de denegación de servicio al sistema a suplantar.

Engaño (spoofing)

Se trata de dar información falsa sobre la identidad del atacante con la finalidad de mantener su anonimato o para tener acceso a sistemas o servicios a los que no podría llegar utilizando su propia identidad. En muchos ataques es común el enmascaramiento de la dirección IP del intruso, esto se conoce como IP spoofing.

Correo no solicitado (spam)

Se trata de mensajes de correo electrónico enviados de forma indiscriminada. Estos mensajes son utilizados a menudo con fines comerciales por compañías de marketing directo. La recepción masiva de este tipo de correo puede constituir un ataque de denegación de servicio, conocido como mail bombing.

Explotación de errores del sistema (bugs)

Cada día se descubren nuevas vulnerabilidades, nuevos fallos en programas y sistemas operativos que pueden ser aprovechados por un atacante para ejecutar código o incluso introducirse en el sistema atacado.

Código malicioso

Se trata de programas que, cuando son ejecutados, causan algún tipo de daño en el sistema sobre el que se ejecutan. En este grupo se engloban virus, caballos de Troya y gusanos, y entre los daños que pueden causar están la pérdida de información, pérdida de capacidad de procesamiento, pérdida de espacio en memoria o incluso la permisión de entrada a un intruso en el sistema.

Ingeniería social

Este tipo de ataque no va dirigido contra un sistema, sino contra una persona, abusando de su bondad, falta de picardía o candidez para obtener cierta información reservada. Es una maniobra que en ocasiones se utiliza para recabar la información que se necesita para un posterior ataque.

2.8. La defensa

2.8.1. Firewall

Tras su aparición, se pensó que el cortafuegos estaba llamado a ser la herramienta de seguridad definitiva. Sin embargo, dado que no bloquea todo el tráfico que lo atraviesa, es posible camuflar un ataque contra un sistema protegido mediante un cortafuego entre el tráfico permitido por éste. A su vez se pueden atacar los servicios de red expuestos e incluso servicios y sistemas no expuestos directamente mediante el túnel de tráfico. De este modo, pese a su innegable importancia en el terreno de la

seguridad informática, los cortafuegos han demostrado ser una medida insuficiente para garantizar al cien por ciento la seguridad de la red que protege.

Hoy por hoy, tras largos años de investigación, no existe aún una herramienta capaz de proteger totalmente una red o un sistema conectado a Internet. Es más, ni siquiera es posible medir con fiabilidad la seguridad de un sistema, y mucho menos de una red. Por tanto, y ante la ausencia de una solución total, la seguridad precisa del empleo de distintas soluciones parciales. El mejor modo de proteger una red es utilizar de manera conjunta distintas técnicas y herramienta.

2.8.2. Diseño de la red

El primer elemento que hay que cuidar es el propio diseño de la red. Teniendo en cuenta las necesidades y las posibles limitaciones de una organización, habrá que estudiar a conciencia las ventajas y los inconvenientes de las distintas topologías, así como de los distintos componentes tanto hardware como software que se pueden utilizar para constituir la red. Una red ha de ser diseñada desde el principio pensando en la seguridad.

2.8.3. Control de usuarios

No se puede descuidar otro factor, los usuarios de una red son una pieza fundamental en la seguridad de una organización. Han de cumplir su parte en la política de seguridad de la empresa, han de conocer las posibles implicaciones que puede tener la utilización de contraseñas inseguras o una mala asignación de permisos a sus archivos y deben de ser conscientes de la necesidad de utilizar criptografía para garantizar la confidencialidad y la integridad de la información privada de la organización en sus conexiones.

Una vez que la red está instalada y configurada y los usuarios cumplen las políticas de seguridad, es el momento de asegurar los sistemas. Esta tarea consiste en deshabilitar las funcionalidades innecesarias, actualizar los sistemas y las aplicaciones y monitorizar de forma periódica los logs registrados tanto por el sistema como por las aplicaciones.

La seguridad informática es un escenario en continuo cambio, a diario aparecen nuevas vulnerabilidades y, lo que hoy es seguro, mañana no tiene por qué serlo. Cada vez que se descubre una vulnerabilidad, los fabricantes y los desarrolladores generan parches y ofrecen actualizaciones que será necesario instalar para reducir el riesgo. Esta constante aparición de vulnerabilidades y soluciones requiere que el administrador se mantenga informado.

2.8.4. Sistemas operativos seguros

Muchos sistemas operativos y aplicaciones, en su instalación por defecto, habilitan puertos y servicios que no se utilizan y que, en ocasiones, ni siquiera se conoce ni su existencia ni su utilidad. Cualquier servicio que no sea estrictamente necesario para el funcionamiento de una organización supone un riesgo y habrá de ser deshabilitado. Cualquier puerto que no sea requerido para el funcionamiento de algún servicio necesario deberá ser cerrado. Cuantas menos facilidades se den a un hipotético intruso, mejor para la seguridad del sistema.

2.8.5. Registros de actividad

Los logs constituyen el registro de la actividad del sistema y de sus usuarios. Por este motivo, albergan las primeras evidencias de actividad no permitida en los equipos, por lo que es necesario consultarlos de manera periódica. Cuando un intruso accede a un sistema, una de sus primeras preocupaciones será el borrado de sus huellas. Para

esto modificará o eliminará los registros y posiblemente trucará el sistema de logs para que no le delate.

Para evitar el borrado y la modificación de registros es recomendable utilizar un servidor remoto de logs instalado en un sistema confiable. Con el empleo del término confiable se pretende remarcar que, aunque por supuesto cualquier sistema es atacable, se habrán de tomar medidas adicionales para dificultar el acceso al sistema por parte de un intruso.

2.8.6. IDS

Un detector de intrusiones es un sistema o conjunto de sistemas que tiene la capacidad de detectar cambios en el estado de un sistema o de una red y que cada vez que detecta algún indicio de ataque registra el incidente y genera algún tipo de alarma o toma alguna medida prediseñada y orientada a proteger la red. Hay dos tipos distintos de detector de intrusiones, los basados en host y los basados en red:

Detectores basados en host: son aplicaciones que monitorizan los logs del sistema, las conexiones de red abiertas o los discos duros del equipo, a la espera de la aparición de indicios de actividad hostil, como algún intento atípico de acceso al sistema o la modificación de algún archivo del sistema.

Detectores basados en red: son sistemas que escuchan y analizan el tráfico que atraviesa un segmento de red buscando patrones conocidos de ataque.

Frente a los basados en host, los basados en red, presentan la ventaja de que, desde un único punto, pueden monitorizar el tráfico de red de multitud de equipos. Así, centralizan la configuración, los registros y las alarmas. Por el contrario sólo son

capaces de reconocer patrones de ataques conocidos, de modo que pueden ser ineficaces frente a nuevas vulnerabilidades.

Otro posible inconveniente se puede derivar de la cantidad de tráfico que tengan que analizar. Si es excesivo pueden recoger demasiada información, dificultando la identificación de información valiosa, o incluso descartando paquetes maliciosos por no poder almacenarlos en el buffer de análisis. Teniendo en cuenta estas limitaciones, ambos tipos de detector de intrusiones son soluciones complementarias que pueden convivir en una red.

2.8.7. Honeypots

Existe otro grupo de herramientas a tener en cuenta en el terreno de la detección de intrusiones, los honeypots. Un honeypot, o señuelo, es un sistema capaz de detectar y registrar los intentos de ataque contra los servicios de red que ofrece. Existen honeypots muy distintos que ofrecen diferente grado de interacción con el intruso. En este sentido las honeynets son los honeypots que proporcionan el nivel más alto. Las honeynets ofrecen al intruso el acceso a una red completa de sistemas reales, y registran todas las acciones que el atacante lleve a cabo en su sistema. Esta capacidad de recopilación de información, junto con su posterior análisis, da a este tipo de honeypot un valor que va mucho más allá de la detección de intrusiones. Se trata de una herramienta de investigación que permite tanto observar en acción las técnicas y herramientas utilizadas por los intrusos, como descubrir nuevas vulnerabilidades utilizadas en los sistemas que forman la honeynet.

2.9. IDS (Sistema de detección de intrusos)

2.9.1. Historia

Cuando las personas escuchan hablar acerca de los Sistemas de Detección de Intrusiones, generalmente se los asocia con alarmas contra ladrones pero con la diferencia que es para computadoras o redes. Es fácil entender este tipo de conceptos con comparaciones o ejemplos sencillos. En realidad, la explicación es bastante aproximada, y los usuarios que no se dedican a la seguridad no necesitan conocer más. Sin embargo, los expertos en este tipo de seguridad no se pueden conformar con conceptos tan triviales y mucho menos cometer errores, sin tener conocimiento alguno sobre la historia de estos sistemas.

La detección de intrusiones es el fruto de la aplicación del Procesamiento Electrónico de Datos (EDP) a las auditorías de seguridad, utilizando mecanismos de identificación de patrones y métodos estadísticos. Es una parte imprescindible en las modernas tecnologías de seguridad de redes.

Antes de la detección de intrusiones existían las auditorías de seguridad. La auditoría es el proceso de generar, almacenar y revisar eventos de un sistema cronológicamente.

La Figura II.4 muestra un esquema simple del funcionamiento de un sistema de auditorías. Los eventos de sistema son capturados por los generadores de auditorías, que llevan los datos al elemento encargado de guardarlos en un fichero de "logs". El analizador, en base a unas políticas de seguridad, emite los resultados a través de un terminal.

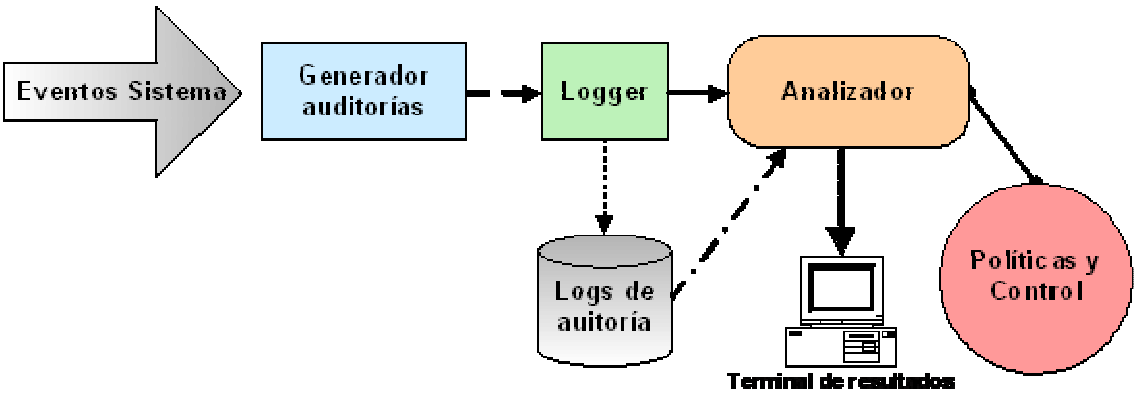

Figura II.4 - Sistema de Auditorías Básico

Durante los comienzos de la historia de los ordenadores, estas máquinas eran relativamente escasas y muy caras. Su uso estaba restringido a técnicos e ingenieros especializados. Los primeros sistemas de auditorías tenían como propósito medir el tiempo que dedicaban los operadores a usar los sistemas que monitorizaban, con una precisión de milésimas de segundo, y servían entre otras cosas para poder facturarles el mismo.

2.9.2. Los primeros Sistemas de Detección de Intrusiones

A medida que el número de ordenadores crecía, el número de eventos de sistema a analizar era tal que esta tarea se volvía humanamente imposible. Las autoridades militares norteamericanas se dieron cuenta de que el uso cada vez más masivo de ordenadores en sus instalaciones requería algún mecanismo que facilitara la labor de los auditores.

James P. Anderson fue la primera persona capaz de documentar la necesidad de un mecanismo que automatizara la revisión de los eventos de seguridad. Describió el concepto de "Monitor de Referencias" en un estudio encargado por las Fuerzas Aéreas de EEUU, y redactó un informe en 1980 que sería el primero de los futuros

trabajos sobre detección de intrusiones. Uno de los objetivos de este informe era la eliminación de información redundante o irrelevante en los registros de sucesos.
Anderson propuso un sistema de clasificación que distinguía entre ataques internos y externos, basado en si los usuarios tenían permiso de acceso o no al ordenador. Estos eran los principales objetivos de los mecanismos de auditoría de seguridad:

- Debían proporcionar suficiente información para que los encargados de seguridad localizaran el problema, pero no para efectuar un ataque.
- Debía ser capaz de obtener datos de distintos recursos de sistema.
- Para evitar ataques internos, debía detectar usos indebidos ("misuse") o fuera de lo normal por parte de los usuarios (o recursos).
- El diseño del mecanismo de auditoría debía ser capaz de obtener la estrategia usada por el atacante para entrar en las cuentas.

Ideó un sistema para dar solución al problema de los intrusos que se habían apoderado de cuentas de usuario legítimas. El cual debía distinguir entre el comportamiento normal o inusual de las cuentas basándose en patrones de uso, creados a partir del análisis de estadísticas de comportamiento de usuario. Los sistemas posteriores trabajarían esta idea.
El "Instrusion Detection Expert System" (IDES), desarrollado entre 1984 y 1986, fue un modelo que definía un sistema de detección de intrusiones en tiempo real. Este proyecto, fundado entre otros por la Marina estadounidense proponía una correspondencia entre actividad anómala y abuso, o uso indebido. Entendiendo por anómala, aquella actividad rara o inusual en un contexto estadístico. Usaba perfiles para describir a los sujetos del sistema (principalmente usuarios), y reglas de actividad para definir las acciones que tenían lugar (eventos de sistema o tiempos de CPU).

Estos elementos permitían establecer mediante métodos estadísticos las pautas de comportamiento necesarias para detectar posibles anomalías. IDES era un sistema híbrido porque añadía un nivel de seguridad adicional mediante el uso de un sistema experto, basado en reglas de seguridad, que minimizaba los efectos de un intruso que intentara eludir el detector de anomalías.

El "Network System Monitor" (NSM) fue desarrollado en la Universidad de California para trabajar en una estación UNIX de Sun. Fue el primer sistema de detección de intrusiones que monitorizaba el tráfico de red, utilizando los datos del propio tráfico como principal fuente de datos. Los anteriores sistemas utilizaban los eventos de sistema o registraban las pulsaciones de teclado. El funcionamiento del NSM, que muchos sistemas de detección de intrusiones de red utilizan hoy en día, se puede describir en estos pasos:

- Ponía el dispositivo de red en modo promiscuo, de forma que monitorizara todo el tráfico que recibiera, incluido el que no iba dirigido al sistema.
- Capturaba los paquetes de red.
- Identificaba el protocolo utilizado para poder extraer los datos necesarios (IP, ICMP, etc.).
- Utilizaba un enfoque basado en matrices para archivar y analizar las características de los datos, en busca tanto de variaciones estadísticas que revelaran un comportamiento anómalo como de violaciones de reglas ya preestablecidas.

Una de las pruebas que se hicieron con el NSM duró dos meses. Monitorizó de 111.000 conexiones, y detectó correctamente más de 300 posibles intrusiones. Como dato significativo, y para enfatizar la necesidad del uso de este tipo de sistemas, hay

que señalar que los administradores no llegaron a percibir ni el 1% de dichas intrusiones.

2.9.3. Tipos de Sistemas de Detección de Intrusiones

Como se ha visto, durante los comienzos de la detección de intrusiones, la mayoría de los sistemas estaban pensados para monitorizar "hosts" (máquinas). Salvo algunas excepciones como el mencionado NSM, que empezó a utilizar el tráfico de red como objetivo de vigilancia.

A partir de los años 90, el rápido crecimiento de las redes de ordenadores hizo que surgieran nuevos modelos de detección de intrusiones. Los daños provocados por el famoso gusano de Internet en 1988, ayudaron a que unieran esfuerzos las actividades comerciales y académicas en busca de soluciones de seguridad en este campo. El primer paso para la fusión de sistemas de detección basados en máquina y red fue el "Distributed Intrusion Detection System" (DIDS). El objetivo inicial del DIDS era proporcionar medios que permitieran centralizar el control y publicación de resultados en un controlador central.

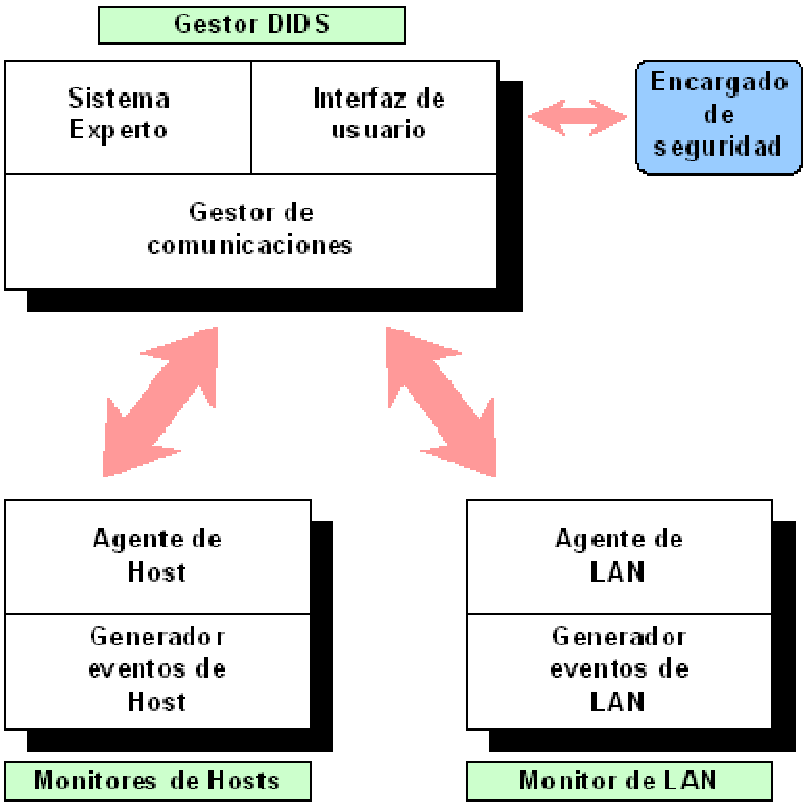

Figura II.5. Sistema de Detección de Intrusiones Distribuido (DIDS)

El DIDS afrontó diversos problemas. Los más importantes estaban con el hecho de tener que registrar eventos asociados a distintas máquinas a lo largo de la red. Un atacante suele aprovecharse de las redes para distribuir sus ataques, realizando éstos desde distintas máquinas. El DIDS fue el primer sistema capaz de relacionar los eventos que recibía para poder detectar una posible intrusión. Además, reunía la información de forma que era posible hacer un seguimiento del posible intruso. Esto permitía su uso para poder ser identificado y perseguido por la ley.

Para solventar el problema de relacionar los eventos que tenían lugar en los distintos niveles de abstracción de la red, el DIDS utilizaba un modelo de detección de intrusiones estratificado en seis niveles que distinguían los distintos tipos de datos.

2.9.4. Términos de seguridad

La detección de intrusiones es el proceso de monitorizar redes de ordenadores y sistemas en busca de violaciones de políticas de seguridad. Los sistemas de detección de intrusiones están compuestos por tres elementos funcionales básicos:

- Una fuente de información que proporciona eventos de sistema.
- Un motor de análisis que busca evidencias de intrusiones.
- Un mecanismo de respuesta que actúa según los resultados del motor de análisis.

La detección de intrusiones es la evolución de las auditorías tradicionales. En términos de seguridad informática, llevar a cabo la auditoría de un sistema significa examinar y analizar el rastro de auditoría que genera el sistema operativo y otros elementos del sistema. La revisión de los eventos se llevaba a cabo entre otros motivos para asegurarse de que no se violaban una serie de políticas de seguridad. Cuando se encontraba alguna irregularidad, surgían nuevos elementos básicos que cubrir:

- **Responsabilidades:** Encontrar el responsable de provocar la violación.
- **Evaluación de daños:** Verificar los problemas provocados en el sistema y de qué forma fueron realizados.
- **Recuperación:** Qué acciones son necesarias para recuperar el estado normal.

A medida que las máquinas se fueron haciendo más rápidas y complejas, el número de sucesos a analizar era tal que no podía llevarse a cabo de la manera tradicional. Por esta razón se desarrollaron mecanismos cada vez más eficaces para simplificar la labor de los auditores de sistemas. Los primeros sistemas que se encargaban de esta labor utilizaban soluciones basadas en técnicas de reducción de eventos y patrones estadísticos.

Antes de hacer que un sistema o red sea seguro, primero es necesario definir lo que se entiende por términos como seguridad, confianza, vulnerabilidad, etc.

2.9.4.1. Seguridad

La seguridad se puede entender desde dos puntos de vista; el práctico y el formal. Desde una perspectiva práctica, un sistema seguro es "aquel con que se cuenta que actúe de la manera esperada". Este punto de vista tiene unas explícitas implicaciones de confianza. Pero la confianza no se puede medir. No podemos confiar en que un sistema se comporte como debe. Nadie nos puede asegurar que un sistema se está comportando como realmente tiene que hacerlo.

Según el enfoque formal, más preciso, la seguridad se define a través de una "tríada de conceptos": confidencialidad, integridad y disponibilidad.

La **confidencialidad** implica que la información sea accedida exclusivamente por el personal autorizado a la misma.

La **integridad** consiste en la necesidad de mantener la información inalterada.

La **disponibilidad** se refiere a la necesidad de ofrecer un servicio ininterrumpidamente, de forma que pueda ser accedido en cualquier momento y desde cualquier lugar, evitando en lo posible que algún tipo de incidencia detenga el mismo.

2.9.4.2. Confianza

Otro aspecto muy importante en la seguridad de sistemas es la confianza. La confianza es la esperanza que se tiene de que un sistema se comporte como realmente debería. Establecer relaciones de confianza sin garantías conlleva la aparición de vulnerabilidades, que se convierten en potenciales amenazas.

2.9.4.3. Vulnerabilidad

Las vulnerabilidades son deficiencias o agujeros de seguridad del sistema que pueden ser utilizadas para violar las políticas de seguridad. Existen muchos tipos de vulnerabilidades. Pueden ser debidas a problemas en el diseño de una aplicación, bien de software o de hardware. O también pueden ser debidas a un plan poco exhaustivo o insuficiente de políticas de sistema.

2.9.4.4. Amenaza

Las amenazas son el resultado de explotar las vulnerabilidades. Una amenaza es una situación que tiene la capacidad de perjudicar o dañar al sistema. Aunque tanto las amenazas como las vulnerabilidades estén muy relacionadas, no son lo mismo. La detección de intrusiones se debe encargar de identificar y responder a ambas.

2.9.4.5. Políticas de seguridad

Las políticas de seguridad son el resultado de documentar las expectativas de seguridad. El concepto de seguridad, como se explicó antes, está relacionado con el comportamiento esperado de un sistema. Se puede afirmar que las políticas de seguridad intentan plasmar de alguna manera en el mundo real, los conceptos abstractos de seguridad. Hay dos formas de definir las políticas de seguridad: procesal (o directiva) y formal.

La política de seguridad procesal consiste en plasmar de forma práctica las ideas o filosofías de la empresa en cuanto a seguridad. Aquí abajo se puede observar el funcionamiento básico de esta forma de entender las políticas de seguridad.

Tabla II.V. Ejemplo de política de seguridad procesal

Política	Procedimiento	Práctica
Necesitamos proteger nuestro servidor Web contra accesos no autorizados.	Se mantendrá actualizado el servidor Web en cuanto a seguridad.	Se comprobará diariamente si existen parches de seguridad del servidor Web, en cuyo caso se aplicarán.
	Se instalará un IDS configurado para comprobar que la actividad en el servidor Web es normal.	Se instalará la última versión del "Snort", y se aplicarán los cambios de configuración pertinentes para concentrar la vigilancia especialmente en el servidor Web

Hay que señalar que los objetivos de la política de seguridad de un sistema son similares a los de los códigos legales. Ambos pretenden proteger a los usuarios legítimos del sistema de los delincuentes. Las políticas de seguridad se escriben en lenguaje informal, no de forma matemática.

Una política de seguridad formal es un modelo matemático del sistema que abarca todos los posibles estados y operaciones así como un esquema de cómo cada estado y operación pueden tener lugar. Definir este tipo de política de seguridad es una ardua labor. Es más apropiada para los diseñadores de sistemas de detección de intrusiones porque, al estar definida de una forma precisa, es más fácil de traducir en patrones de detección. Además, esta forma de describir el sistema ayuda al diseñador a escoger el tipo de información que se debe recopilar para el análisis.

2.9.4.6. Elementos de la infraestructura de seguridad

Aunque la detección de intrusiones pueda ser uno de los sistemas más importantes en el ámbito de la seguridad, no es la solución definitiva. Existen otros elementos que ayudan en la labor de mantener un sistema seguro, sin los cuales no se podría obtener un nivel apropiado de fiabilidad. En una instalación física segura, como un edificio, se utilizan materiales robustos para su construcción. Se sitúan ventanas de forma que no sean fácilmente accesibles por ladrones. Se colocan barreras y controles de acceso alrededor de la instalación. En el interior, además, se dispone de sistemas de vigilancia y alarmas, así como de personal debidamente equipado que patrulla continuamente la instalación. Este tipo de protección se encuentra a diario en bancos o instalaciones militares.

Pues bien, esto mismo ocurre con los ordenadores y las redes de datos. Hay numerosos componentes y funciones que forman parte del intrincado plan de estrategias de protección de un sistema. Algunos de los cuales se comentan a continuación.

2.9.4.6.1. Control de acceso

El control de acceso restringe el acceso a objetos según los permisos de acceso del sujeto. Se divide en Control de Acceso Obligatorio (MAC), en el que los permisos de acceso los proporciona el sistema; y el Control de Acceso Discrecional (DAC), en el que los permisos de acceso los controla y configura el propietario del objeto.

2.9.4.6.2. Identificación y Autenticación

Los mecanismos de identificación y autenticación (I&A) posibilitan la identificación adecuada de sujetos y objetos al sistema. Estos elementos se pueden dividir en tres categorías, dependiendo de los datos que necesiten: lo que sabes, lo que tienes, lo que eres. Todas y cada una de las categorías implica un secreto que sólo conocen el

sistema y el usuario. Si el secreto del usuario coincide con el que guarda el sistema, se valida la identidad del usuario y se obtiene permiso de acceso al sistema.

"Lo que sabes" se corresponde con el mecanismo básico de I&A, en el que cada sujeto se identifica y autentifica con un nombre de usuario y una contraseña. Desgraciadamente, este mecanismo ha demostrado ser ineficaz ante varios ataques, como "password-crackers" (rompedores de contraseñas) o troyanos que capturan actividad de teclado. Esta técnica de autenticación está siendo lentamente reemplazada por otras más robustas, de conocimiento cero que evitan el acto de pasar el secreto en sí mismo.

La siguiente categoría, "lo que tienes" se puede ejemplificar claramente en sistemas "token-based" (basados en testigos), tales como los que necesitan el uso de una tarjeta inteligente, una clave ("key"), un disco especial. Muchos de estos testigos se han diseñado para utilizar medios criptográficos y soportes físicos resistentes para protegerse de ataques o suplantaciones de identidad (enmascaramiento).

Por último "lo que eres" representa a los mecanismos de I&A que utilizan elementos biométricos tales como la voz, huellas dactilares, o retina. Los procesos de autenticación también se utilizan para proporcionar seguridad, y no sólo para dar acceso al sistema a los usuarios. Además, también sirven a los sistemas de detección de intrusiones para detectar si los comportamientos sospechosos son iniciados por usuarios legítimos o intrusos.

2.9.4.7. Cifrado

El cifrado es probablemente el método más antiguo utilizado para proteger información. No sólo permite ocultar información a sujetos no autorizados, sino que permite detectar posibles alteraciones, intencionadas o accidentales, en la misma.

El cifrado es el proceso por el cual un documento en claro, sometido a un algoritmo de cifrado con una clave, da lugar a un documento cifrado. Aunque el cifrado protege en

gran medida la información, no puede evitar que sea eliminada de forma malintencionada. No puede proteger el documento antes de ser cifrado ni después de ser descifrado. Además, es completamente inútil si la clave es descubierta.

2.9.4.8. Cortafuegos

Los cortafuegos proporcionan una barrera de seguridad entre redes de distintos niveles de confianza o seguridad, utilizando políticas de control de acceso de nivel de red. Los elementos que entran en este grupo son por ejemplo los servidores "proxy", filtros de paquetes de red, túneles de datos cifrados (también conocidos como Redes Privadas Virtuales (VPN)). Los cortafuegos filtran paquetes de red, permitiendo o denegando su paso según las políticas establecidas. También hacen traducciones de direcciones, permitiendo mantener oculta la configuración interna de una red local.

2.9.5. Elementos de un IDS

2.9.5.1. Arquitectura

A la hora de proteger un sistema basándose en los registros que se analizan mediante una auditoría requiere que estos registros sean almacenados de una forma segura en un entorno distinto al del sistema protegido. Este requisito lo cumple cualquier sistema de detección de intrusiones con un mínimo de calidad. Esto se hace por varias razones. Para evitar que el intruso pueda eliminar los registros, para evitar que el intruso pueda alterar la información contenida en los registros y para no perjudicar con el mecanismo de detección de intrusiones el rendimiento del sistema a proteger.

En este tipo de arquitectura el sistema que ejecuta el sistema de detección de intrusiones se denomina "host" y el sistema monitorizado "target" (objetivo).

2.9.5.2. Fuentes de datos y monitoreo

La fuente de datos es una de las primeras cosas a tener en cuenta a la hora de diseñar un sistema de detección de intrusiones. Estas fuentes se pueden clasificar de muchas maneras. En lo que respecta a la detección de intrusiones las clasificaremos por localización. De esta forma, la monitorización de sistemas, y por tanto la detección de intrusiones, se puede dividir en cuatro categorías: host", red, aplicación y objetivo. Usaremos el término "monitorizar" como el acto de recoger datos de una determinada fuente y enviarlos a un motor de análisis.

- **Monitores basados en máquina ("host based"):** Recogen los datos generados por un ordenador, normalmente a nivel del sistema operativo. Los registros de sucesos y las colas de auditoría pertenecen a este grupo.

- **Monitores basados en múltiples máquinas ("multi-host based"):** Como su propio nombre indica, utiliza la información recogida en dos o más máquinas. Su enfoque es muy similar al basado en máquina, con la dificultad añadida de tener que coordinar los datos de varias fuentes.

- **Monitores basados en redes ("network based"):** Capturan paquetes de red. Para ello, normalmente se utilizan dispositivos de red en modo promiscuo, convirtiendo al sistema en un "sniffer" o rastreador.

- **Monitores basados en aplicación ("application based"):** Registran la actividad de una determinada aplicación. Por ejemplo, los registros de un servidor ftp.

- **Monitores basados en objetivos ("target based"):** Estos monitores difieren ligeramente del resto porque generan sus propios registros. Utilizan funciones de cifrado para detectar posibles alteraciones de sus objetivos, y contrastan los resultados con las políticas. Este método es especialmente útil cuando se usa contra elementos que, por sus características, no permiten ser monitorizados de otra forma.

- **Monitores híbridos ("hybrid"):** Combinan dos o más fuentes de distinto tipo. Cada vez es más frecuente encontrarse con productos de detección de intrusiones basados en este punto de vista. Así, amplían sus posibilidades de detección.

Existen productos que combinan varias estrategias de monitorización. Estas soluciones se denominan soluciones integradas.

Hay que añadir que existen sistemas de detección de intrusiones que reciben el nombre de NNID ("Network Node Intrusion Detector"), es decir, Detector de Intrusiones de Nodo de Red. En realidad, son un caso especial de la detección basada en red. Este nombre se aplica cuando el monitor basado en red se sitúa en un "host", monitorizando los paquetes destinados u originados por la máquina anfitriona. Una de las razones más importantes para hacer esto es para sortear el problema de

las encriptaciones durante la comunicación, ya que el tráfico es cifrado o descifrado por el propio "host". Un detector basado en red convencional no podría analizar el tráfico en un punto intermedio entre dos nodos que cifraran sus comunicaciones. Los NNIDS son también útiles en entornos de red con conmutadores ("switches") en los que un "host", aunque esté en modo promiscuo, sólo percibe el tráfico destinado a él.

2.9.5.3. Tipos de análisis

Después del proceso de recopilación de información, se lleva a cabo el proceso de análisis. La detección de intrusiones también se puede clasificar según los objetivos del motor de análisis. Los dos tipos principales de análisis son:

- **Detección de usos indebidos ("misuse"):** Para encontrar usos indebidos se comparan firmas con la información recogida en busca de coincidencias.
- **Detección de anomalías:** Para la detección de anomalías se manejan técnicas estadísticas que definen de forma aproximada lo que es el comportamiento usual o normal.

La figura II.6. Muestra un esquema general de detector de intrusiones de usos indebidos (mediante comparación de patrones) y de anomalías.

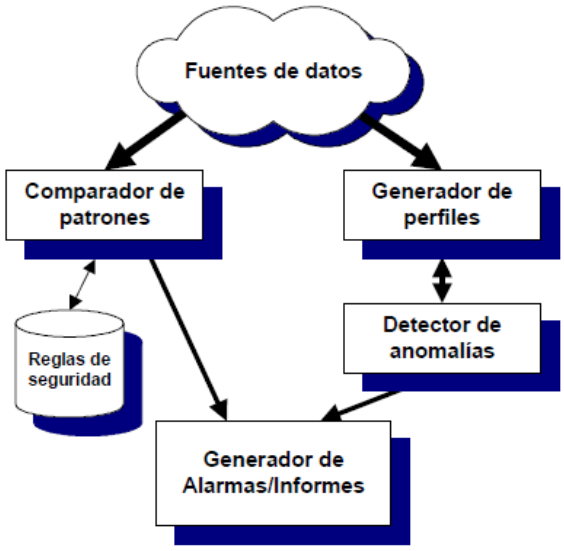

Figura II.6. Esquema general de un Sistema de Detección de Intrusiones

La mayoría de los detectores son de usos indebidos, anomalías o una mezcla de ambos. Algunas empresas están empezando a utilizar también técnicas específicas para la detección de ataques de denegación de servicio (DoS), dadas sus características especiales.

Aparte del análisis basado en firmas y estadísticas, también existe el análisis de integridad. Este es el método utilizado por las herramientas de chequeo de integridad de ficheros, que complementan a los Sistemas de Detección de Intrusiones. Estas herramientas detectan cambios en ficheros u objetos, utilizando mecanismos robustos de encriptación tales como funciones resumen ("hash functions").

Otro enfoque a la hora de distinguir formas de detección de intrusiones es teniendo en cuenta el uso que hacen los análisis del tiempo:

- **Por lotes ("batch mode"):** Cada intervalo de tiempo se procesa una porción de los datos recibidos, enviando las posibles alarmas de intrusiones después de que hayan ocurrido.
- **Tiempo real:** Los datos son examinados en el tiempo en que son recibidos (o con un retardo mínimo). La aparición de los análisis en tiempo real hizo posible las respuestas automáticas.

2.9.5.4. Respuestas

El mecanismo de respuesta, es otro de los factores que ayudan a definir el tipo de sistema de detección de intrusiones:

- **Respuestas pasivas:** En este caso, el detector no toma acciones que puedan cambia r el curso de un ataque. En vez de esto, se limita a enviar o registrar la alarma correspondiente al responsable cualificado.
- **Respuestas activas:** Pertenecen esta categoría aquellos sistemas que, además de generar la alarma correspondiente, reaccionan modificando el entorno. Un ejemplo de este tipo de respuesta activa consiste en el bloqueo de las acciones del intruso, o el cierre de la sesión del usuario sospechoso.

CAPÍTULO III

3. ANÁLISIS CUALITATIVO Y CUANTITATIVO DE LAS HERRAMIENTAS HONEYPOTS

3.1. Introducción

Actualmente en el mundo de la informática, unos de los puntos claves son las redes de computadores debido a que permite el manejo de datos e información en todas las empresas y organizaciones de manera oportuna y veraz.

La aparición en los últimos años de las redes informáticas y fundamentalmente de Internet, ha sido el factor fundamental que ha hecho que la Seguridad Informática cobrase una importancia vital en el uso de sistemas informáticos conectados. Desde el momento en que nuestro ordenador se conecta a Internet, se abren ante nosotros toda una nueva serie de posibilidades, sin embargo estas traen consigo toda una serie de nuevos y, en ocasiones complejos tipos de ataque. Dichos ataques pueden ser caracterizados como anomalías en el comportamiento usual del flujo de datos en dicha red de comunicaciones.

La presente investigación se basa en la implementación de un sistema de detección y análisis de intrusiones no autorizadas en la red, haciendo uso de herramientas de los sistemas llamados Honeypots para la cual hemos visto necesario seleccionar las mejores herramientas que permitan obtener un sistema más confiable y seguro

mediante un estudio comparativo de las herramientas honeypots que se encuentran disponibles en la actualidad.

En el presente capítulo se realizará el estudio comparativo de las herramientas honeypots, basándonos en ciertos parámetros, con el fin de determinar cual brinda las mejores prestaciones dando así una base que permitirá seleccionar la herramienta más adecuada para el desarrollo de sistemas de intrusos en la red mediante Honeypots acorde a las necesidades de la institución.

3.2. Determinación de las herramientas a comparar

En la actualidad existe gran variedad de herramientas para sistemas honeypots, tanto comerciales como open source, entre las más importantes podemos citar las siguientes:

Honeyd, BOF, Detection ToolKit (DTK), Sebek, KFSensor, Specter, Sysmantec Decoy Server, todas estas de gran importancia para le detección de intrusos en la red. Sin embargo se ha creído conveniente realizar el análisis cuantitativo y cualitativo de 3 de estas herramientas, ya que consideramos son las de mayor uso, por las siguientes razones:

- En la siguiente url http://comunidad.dragonjar.org/f155/redes-trampa-honeypots-de-baja-interaccion-7926/, donde destaca las redes trampa (Honeypots de baja interacción) señala como las principales herramientas para un sistema honeypot las siguientes:
  - ✓ Honeyd
  - ✓ BOF
  - ✓ HoneyBoth
  - ✓ Specter

Recalcando las características de Espector como unos de los programas comerciales más completos honeypots de baja interacción, a honeyd como una excelente herramienta open source que funciona prácticamente en cualquier plataforma.

- En el sitio oficial de insecure, con el siguiente enlace: http://insecure.org/tools/tools-es.html, en la lista de las 75 herramientas de seguridad más utilizadas, se destaca a Honeyd como la mejor herramienta para detección de intrusos en la red.

- En el sitio de la Universidad Técnica Particular de Loja (UTPL) en el apartado de seguridad de la institución nombra a:
  - ✓ Honeyd
  - ✓ Sysmantec Decory Server (Man Trap)
  - ✓ BOF
  - ✓ Specter

Como las principales herramientas para el desarrollo de sistemas de detección de intrusos en la red.

- En el libro “Honeypots: Tracking Hackers” en el capítulo 5 Classifying Honeypots by Level of Interaction se me menciona a las siguientes herramientas como las más utilizadas en los sistemas honeypots:
  - ✓ Specter
  - ✓ Honeyd
  - ✓ Homemade
  - ✓ BOF

- En la encuesta realizada a 10 personas que manejan aspectos de seguridad en la red (Anexo1) que trabajan en distintas empresas e instituciones y están inmersos con el desarrollo de sistemas Honeypots web nos dieron a conocer cuáles son sus preferencias en cuanto a estas herramientas obteniendo los siguientes resultados.
  - ✓ Honeyd 65%
  - ✓ Specter 20%
  - ✓ DTK 10%
  - ✓ BOF 4%
  - ✓ otras. 1%

Según los datos anteriormente mencionados hemos visto necesario realizar el estudio comparativo con las 3 herramientas más usadas en la actualidad en sus últimas versiones, como son: Honeyd, Espector y BOF. Las tres son herramientas de detección de intrusos en la red que gozan de una gran popularidad, además que cuentan con una amplia gama de recurso para su uso.

3.3. Análisis de las herramientas seleccionadas

3.3.1. Honeyd

Honeyd es desarrollado y mantenido por Niels Provos de la Universidad de Michigan, es OpenSource pre empaquetados un honeypot diseñado para la plataforma Unix. OpenSource significa que la solución es libre, y se tiene acceso a la fuente, que se la puede personalizar. Se ha concebido como una solución de baja interacción, no hay sistema operativo destinado a un atacante para obtener acceso a los servicios emulados.

Honeyd está diseñado principalmente como un honeypot de producción, utilizado para detectar ataques o actividades no autorizadas. Sin embargo, sí tiene aplicaciones

específicas para la investigación, como una solución OpenSource, se puede personalizar el honeypot, tal como el diseño de sus propios servicios emulados. Esto significa que el honeypot puede escuchar en cualquier puerto que desee, Honeyd detecta la actividad en cualquier puerto TCP, emulando servicios que están diseñados sólo para engañar a los atacantes y capturar su actividad.

Honeyd introduce varios conceptos nuevos al mundo de los honeypots. En primer lugar, no detecta los ataques contra su propia dirección IP, como Specter lo hace. En cambio, Honeyd asume la identidad de cualquier dirección IP que no tiene un sistema válido. Cuando un atacante intenta conectarse a un sistema que no existe, Honeyd recibe el intento de conexión, asume la identidad del inexistente sistema y, a continuación, las respuestas al atacante. (Por "no existe" se referie a una dirección IP que no se ha asignado a un sistema y no se utiliza para cualquier propósito.) A partir de ese momento Honeyd comunica al agresor como la víctima del sistema. Honeyd puede supervisar inexistentes millones de direcciones IP para las conexiones. También puede asumir simultáneamente las direcciones IP de miles de víctimas y de interactuar activamente con los atacantes. Honeyd tiene probado más de 60.000 direcciones IP al mismo tiempo. Lo más probable es que su red, y no su honeypot, se convertirá en el cuello de botella en estos casos. Esto significa que puede controlar Honeyd extremadamente grandes redes que no cuentan con los sistemas existentes.

Lo que también es emocionante es que Honeyd puede emular diferentes sistemas operativos al mismo tiempo. Si bien Specter puede emular 13 diferentes sistemas operativos, sólo puede hacer un sistema de una sola vez. Honeyd puede emular muchos sistemas diferentes al mismo tiempo. Por ejemplo, si selecciona su Honeyd para emular un sistema servidor Windows NT 4.0 Server SP5-SP6, no sólo emula los servicios, como un servidor Web de IIS, pero también la IP. En este caso, si usa Nmap para el período de investigación de huellas dactilares, la respuesta será la IP de

Windows NT 4.0 Server SP5-SP6. Esta capacidad se limita actualmente a 473 diferentes tipos de sistemas operativos y versiones.

3.3.1.1. Valor de Honeyd

Como honeypot de baja interacción, Honeyd es principalmente un honeypot de producción, utilizados para detectar los atacantes. Su modelo para la detección es el mismo que la mayoría de honeypots de baja interacción. Cuando se realiza una conexión a un puerto que está escuchando, registra la actividad del atacante se captura, y se genera una alerta. Debido a que los distintos servicios en los puertos tienen un cierto nivel de emulación, en la que el atacante puede capturar la interacción con el servicio.

3.3.1.2. Ventajas de Honeyd

Honeyd tiene 2 ventajas que aumentan su valor:

- La primera es que puede detectar conexiones en cualquier puerto TCP. Los servicios emulados no son necesarios para la detección, ya que existe sólo para la interacción con los agresores y para obtener más información. Esto hace más sencillo el despliegue de Honeyd, y aumenta su capacidad de detección.

- La segunda ventaja a Honeyd es que se puede modificar los servicios emulados y el nivel de interacción. Como una solución OpenSource, la gente en toda la comunidad de seguridad puede contribuir al código Honeyd, incluyendo los servicios emulados. Dado que estos esfuerzos son compartidos entre la comunidad de seguridad, Honeyd puede utilizar un mayor número de servicios con amplios niveles de interacción y la emulación. Con el tiempo,

Honeyd tiene la capacidad para detectar y capturar a los ataques que puedan aumentar exponencialmente. Sin embargo, los servicios emulados sólo se limitan a TCP. No hay servicio de emulación de servicios UDP. Además, con ICMP, Honeyd es limitado a solicitudes de eco ICMP y ICMP ECHO REPLY. No interactuar con cualquier otra actividad basada en ICMP.

- El mayor valor de Honeyd no es el que escucha en los puertos o el nivel de emulación, es su capacidad para controlar a millones de direcciones IP al mismo tiempo. Los honeypots sólo puede controlar la dirección IP asignada a la honeypot. Las posibilidades de detectar un ataque se ven limitados por el número relativamente reducido de direcciones IP controladas. Honeyd no comparte esta limitación. Tiene la capacidad para controlar a millones de direcciones IP y la capacidad de reclamar activamente miles de direcciones IP, todas al mismo tiempo. Se podría pensar que tener que vigilar a millones de direcciones IP Honeyd haría muy complicado la configuración y el despliegue. Tener que identificar a cada dirección IP que se escucha en Honeyd de los ataques requiere tiempo. Honeyd resuelve este problema no escucha en direcciones IP específicas. En cambio, Honeyd monitorea toda la red de bloques de direcciones IP que no están siendo utilizadas. Cuando un intento de conexión se hace a una dirección IP que no tiene sistema de conexión, se remite a la Honeyd honeypot. la conexión, asume la dirección IP de la víctima, y las respuestas al atacante. A partir de ese momento, la interacción entre el atacante y Honeyd es la misma que con cualquier otro honeypot. Conceptualmente, “Honeyd tiene la idea de un honeypot y lo aplica a toda una red”.

3.3.1.3. Funcionamiento de Honeyd

Cuando una dirección IP de un sistema inexistente es atacado, Honeyd asume la identidad de la víctima e interactúa con el atacante. No lo hace mediante la asignación de miles de direcciones IP a sí mismo a la vez. Si no, solo una dirección IP: la dirección IP asignada a su interfaz única. Esta es la misma interfaz que se utiliza para administrar el honeypot. Es la misma interfaz que se encuentra en la red y los monitores de actividad sospechosa.

Honeyd trabaja en el principio de que cuando recibe una conexión de un sistema que no existe, se da por supuesto que el intento de conexión es hostil, muy probablemente una conexión de exploración o ataque. Honeyd cuando recibe dicho tráfico, que asume la dirección IP del destino (lo que la víctima). A continuación, comienza una emulación de servicios para el puerto que está intentando la conexión. Una vez que el servicio emulado se inicia, empieza a interactuar con el atacante y capta toda la actividad. Al momento de salir el atacante termina la interacción y Honeyd continua esperando a recibir más tráfico o los intentos de conexión a los sistemas que no existen. Honeyd asume una dirección IP y se ejecuta un servicio, un método muy eficaz.

Cuando Honeyd recibe más ataques repite el mismo proceso de asumir la dirección IP de la víctima para poder interactuar con él, empieza a emular los respectivos servicios y a capturar el ataque y finalmente salir.

El truco con Honeyd es conseguir que el honeypot reciba el tráfico de sistemas inexistentes pero ¿Cómo se sabe que los sistemas no existen, y cómo el Honeyd recibe esa actividad? Honeyd no identifica activamente inexistentes sistemas, ni vía activamente este tipo de ataques a sí mismo. En lugar de ello, se tiene que obtener el tráfico a la inexistencia de sistemas del Honeyd. Hay dos maneras de hacer esto:

a) El primer enfoque es blackholing (Técnica que permite a un sistema honeyd emular máquinas virtuales sobre peticiones a IPs no existentes), cuando quieras Honeyd para controlar toda una red que no tiene sistemas activos. Esto significa que independientemente de la dirección IP del atacante es la orientación dentro de una red específica, usted sabe que es un ataque, porque la red no tiene los sistemas vivos. Por lo tanto, ponemos la ruta del tráfico de toda la red directamente al Honeyd.

b) El segundo método es que el Honeyd reside en una red que tiene validez y no existen sistemas. La mayoría de las redes de producción en las organizaciones son como esta. Tienen sistemas válidos, pero en cualquier momento hay sin asignar direcciones IP dentro de esa red. El objetivo es transmitir el tráfico de todos los sistemas al inexistente Honeyd.

Blackholing

De los dos métodos que transmita a Honeyd tráfico, la primera es mucho más fácil. Si hay una red que no tiene los sistemas de producción, simplemente tiene que toda la red dirigida a la Honeyd honeypot. Para ello, se agrega una declaración de enrutamiento de un router para dirigir el tráfico de toda la red para el honeypot, de forma similar a cómo agregar una ruta para una declaración de toda la red. En Figura III.7 vemos un diagrama de red de cómo un honeypot Honeyd podría ser utilizado para recibir el tráfico de toda una red inexistente. El comando de configuración utilizado en un router de Cisco para enrutar todo el tráfico de una red para el Honeyd es el siguiente.

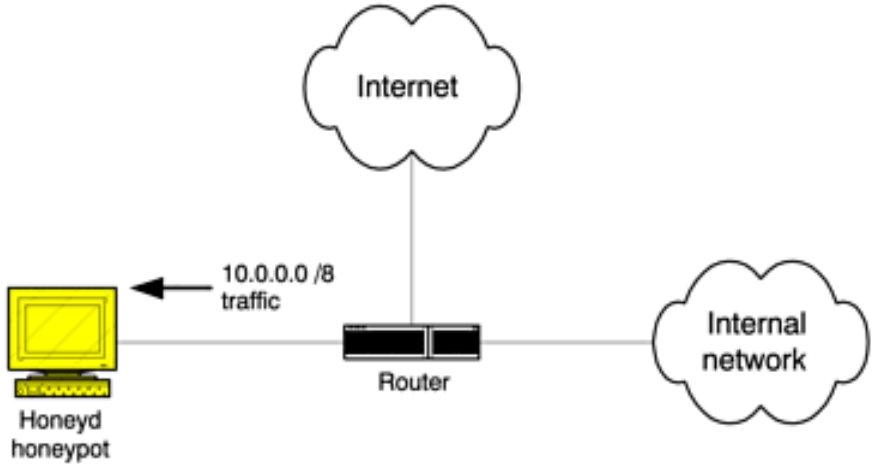

Figura III.7. Diagrama de red demostrando cómo todo el tráfico de una red específica (10.0.0.0 / 8) se redirige al Honeyd.

En este ejemplo, supongamos que la red en cuestión es la red de clase A (más de 16 millones de sistemas), identificado como el 10.0.0.0 / 8 y la red la dirección IP de la Honeyd honeypot es 10.1.1.1. No hay sistemas en esta red, todas las direcciones IP están no asignadas. Por lo tanto, si el Honeyd recibe el tráfico de esta red, es sospechoso por naturaleza, y que interactúa con Honeyd.

Ahora, cuando la organización recibe el tráfico de red destinado a la 10.0.0.0 / 8, el tráfico es transmitido por el router al Honeyd. El honeypot simplemente lo recibe e interactúa con el atacante.

ARP Spoofing

El segundo método de transmisión de tráfico es más complejo. El objetivo del segundo método es para que Honeyd a resida en una red que tiene validez y donde no existen sistemas. En este caso, no podemos tener todo el tráfico de la red siendo enviado al honeypot, ya que la mayoría de tráfico es válida y tiene

que ir a su destino. Como se dijo anteriormente, Honeyd no tiene la capacidad para identificar los sistemas inexistentes, sino que depende de las direcciones IP para llegar al honeypot. En cambio, para la identificación dinámica de sistemas inexistentes, Honeyd depende de otro programa: la utilidad Arpd.

Arpd, identifica los sistemas inexistentes y, a continuación, emite a Honeyd las conexiones, utilizando un método llamado ARP Spoofing. Para el caso de Honeyd, ARP Spoofing es cuando la dirección IP de un sistema inexistente está obligado a la dirección MAC del Honeyd. El resultado final es que, independientemente de la dirección IP del sistema inexistente, el paquete va al Honeyd. Al igual que en el método anterior, una vez que recibe el paquete Honeyd, asume la dirección IP de la víctima e interactúa con el atacante.

3.3.1.4. Respuesta a los ataques

Una vez que el atacante recibe la conexión inicial de Honeyd, a través de blackholing o ARP Spoofing, Honeyd asume la identidad de la víctima y se hace cargo de la conexión. Honeyd identifica entonces ¿a qué puerto se dirige el atacante y reacciona sobre la base de ese puerto?. Una de las varias cosas que puede suceder sería:

a) En primer lugar, Honeyd puede no tener un servicio para el emulador de puerto, en cuyo caso puede responder que el puerto está cerrado, o no puede responder en absoluto, dependiendo de cómo configurar el sistema. Sin embargo, en ambos sentidos Honeyd detecta que intentó, lo que permite a Honeyd detectar la actividad en cualquier puerto.

b) En segundo lugar, Honeyd puede ser configurado para interactuar con el atacante utilizando un servicio emulado. Por ejemplo, si un atacante se conecta

al puerto TCP 111, el honeypot puede simplemente responder con un paquete RST (termina la conexión sin esperar respuesta), declarará cerrado el puerto y luego el intento de registro. Sin embargo, si un atacante se conecta al puerto TCP 80, el honeypot puede iniciar un emulador de servidor Web e interactuar con el atacante, y realizar la captura de sus actividades.

Honeyd tiene la habilidad única de emular sistemas operativos no sólo en el nivel de aplicación, sino también en el nivel IP. Cuando un atacante se comunica con una emulación de servicios, tales como el servidor Web, el servicio emulado se comporta de manera diferente, dependiendo del sistema operativo. Con Specter, el servidor Web Microsoft IIS se convierte en un servidor Web o servidor web Apache, sobre la base del sistema operativo emulado fue basado en Microsoft o Unix. Honeyd tiene la misma capacidad. Sin embargo, con Specter, las IP se basa en la plataforma instalada. Honeyd no tiene esta limitación. Si está emulando un sistema Linux, la IP puede actuar como una pila de propiedad intelectual de Linux, si el Honeyd emula un router de Cisco, también lo puede hacer.

Nmap es una de las herramientas más comunes utilizadas para determinar el tipo de sistema operativo. Nmap envía una serie de paquetes hacia un objetivo, captura la respuesta a los paquetes, y compara la respuesta a una base de datos de firmas conocidas. Sobre la base de las firmas o direcciones IP que se pongan en oferta, podemos determinar el tipo de sistema operativo remoto. Honeyd tiene la misma base de datos de firmas y respuestas a la base del sistema operativo emulado que usa Nmap. Esto significa que si el sistema Honeyd emula un servidor de Windows XP, y es probado por Nmap, Honeyd mira la base de datos de Nmap, determina que servidor

de Windows XP y, a continuación, las respuestas con las IPs. El atacante se hace a la falsa idea que tiene un sistema Windows XP sobre la base IP.

Este método no es infalible. Nmap es uno de las muchas maneras de determinar el tipo de sistema operativo. Otro método es OS huellas dactilares. Estos otros métodos pueden ver a través de la emulación IP del Honeyd y determinar la verdad. Sin embargo, Honeyd mitiga en gran medida el riesgo de la toma de huellas dactilares utilizando Nmap, la base de datos, ya que esta es una de las herramientas más comunes utilizadas para la toma de huellas dactilares.

La otra ventaja de usar la base de datos es como Nmap actualiza y mejora la base de datos de firmas conocidas, Honeyd puede simplemente copiar y utilizar la última base de datos de archivos, mantenerse al día con los nuevos métodos de sondeo.

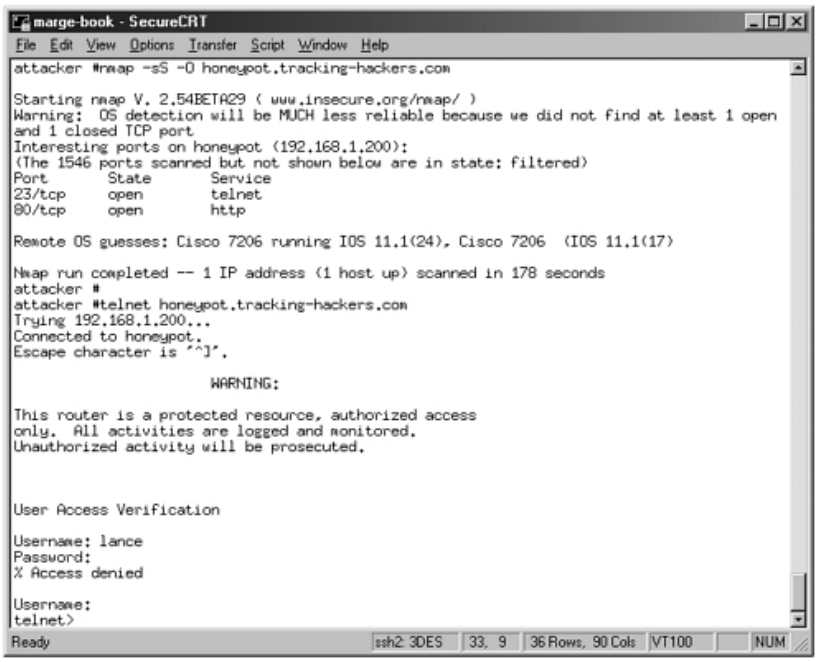

Figura III.8. Ataque con Nmap

En la figura vemos a un atacante utilizando Nmap tomando las huellas dactilares (Con la opción "O"). Nmap activa el sistema de sondas, determina qué puertos están abiertos y a continuación, envía una gran variedad de paquetes para determinar el tipo de sistema operativo. Nmap determina el sistema remoto como un router Cisco, el atacante entonces realiza un Telnet al router y obtiene una entrada con un rótulo de advertencia, al igual que podría esperar de un enrutador de Cisco. El atacante intenta un solo intento de acceso y, a continuación, cierra la conexión. Honeyd demuestra su capacidad de emular, tanto en el IP y el nivel de aplicación.

3.3.1.5. Instalación y configurar Honeyd

Como una solución diseñada OpenSource para Unix, Honeyd no proporciona ningún tipo de apoyo o de una agradable interfaz gráfica para la instalación o configuración. En lugar de ello, descargar el código fuente, compilar el código fuente y, luego, instalar los archivos Honeyd de configuración. Después de ello, ejecutar el Honeyd binario desde la línea de comandos, usando los dos archivos de configuración, a la red que desea. Una vez iniciado, Honeyd debe interactuar con cualquier ataque que se envié por su camino. El comando para iniciar Honeyd es el siguiente:

Honeyd –p /etc/Honeyd/nmap.prints –f etc/Honeyd/honeyd.conf 192.168.1.0/24

El primer comando que está ejecutando Honeyd es la opción -p es la ubicación del archivo de huellas dactilares Nmap. Esta es la base de datos de las firmas utilizadas por Honeyd para emular diferentes sistemas operativos en el nivel IP. Si un atacante utiliza Nmap a la huella dactilar de su sistema operativo, Honeyd Nmap utilizará la base de datos de huellas dactilares para determinar cómo responder al ataque, sobre la base del sistema operativo que están emulando. La segunda opción -f, que es la

ubicación del archivo de configuración Honeyd. Este archivo de configuración que determina los servicios a los que va a imitar y el tipo de sistema operativo.

La última opción es la red que desee supervisar. Esto significa que cada vez que recibe un paquete Honeyd para un sistema inexistente, y la dirección IP pertenece a la red de seguimiento, Honeyd asumirá la identidad de la dirección IP de destino e interactuará con el atacante. Si no se da la dirección de red, Honeyd van a interactuar con cualquier dirección IP enviado a su camino.

El fichero de configuración de Honeyd es sencillo, pero tiene una gran cantidad de opciones. Este en un ejemplo simple de cómo poder hacer un archivo de configuración para nuestro Honeypot:

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

create windows
set windows personality "Windows NT 4.0 Server SP5-SP6"
set windows default tcp action reset
set windows default udp action reset
add windows tcp port 80 "perl /etc/honeyd/scripts/iis/main.pl"
add windows tcp port 25 block
add windows tcp port 23 proxy real-server.tracking-hackers.com:23
add windows tcp port 22 proxy $ipsrc:22
set windows uptime 3284460

# bind specific IP addresses to specific templates
bind 192.168.1.200 windows
```

Honeyd trabaja con la creación de plantillas que definen las características de un honeypot, incluyendo tipo de sistema operativo, los puertos que escuchan, y el comportamiento de los servicios emulados. Cada plantilla se le da un nombre.

3.3.2. BackOfficer Friendly

Otra de las herramientas de análisis de los honeypots es BackOfficer Friendly, a menudo llamado HBO. Este es uno de los honeypots simple de usar. Su funcionalidad es muy fácil de entender y configurar. Su sencillez es lo que hace BOF como una excelente herramienta, por ende una gran trampa. Prácticamente cualquier persona puede utilizar BOF.

Al igual que un virus informático, se distribuye como un programa integrado en utilidades shareware descargable y ejecutable de los programas de tarjetas de felicitación. El usuario abre el archivo descargado Back Orifice se instala en la máquina del usuario y permite al atacante el control total del ordenador a través de la conexión a Internet.

El siguiente es un extracto de la documentación BOF que viene con el software

“BackOfficer Friendly es una aplicación de servidor de suplantación de identidad que se ejecuta en el sistema Windows o UNIX , y te avisa cada vez que alguien intenta el control remoto del sistema mediante Back Orifice . Básicamente, se hace pasar por un servidor de Back Orifice . BackOfficer Friendly da las respuestas atacante falsos que parecen que vinieron de Back Orifice , al registrar la dirección los atacantes IP de y las operaciones que intentó realizar.”

Back Orifice fue un troyano muy controvertido y potente desarrollado y publicado por los CDC en Defcon 6 de agosto de 1998. Cuando este troyano se instala en el ordenador de la víctima, el troyano se oculta y permite al atacante el control completo es decir tiene el control remoto del sistema. Un atacante podría controlar todas las actividades de la víctima, como su teclado, copiar todos sus archivos, e incluso volver

a configurar el equipo. Una vez instalado, el atacante va a tener un mayor control del equipo afectado que incluso el propio usuario. Sin embargo, Back Orifice fue mucho menor en tamaño en bytes y el sistema de control es mucho mayor, además no cuesta nada. No era la funcionalidad de la herramienta la que causó tanta controversia, su intención era con fines específicamente para dar a los atacantes el control completo de los sistemas sin que la víctima lo sepa.

La simplicidad de esta herramienta significa que casi cualquier atacante podría utilizar, independientemente de sus conocimientos técnicos o experiencia. Es sin complicaciones que el troyano infecta un ordenador, la herramienta tenía un cliente interfaz gráfica de usuario simple, dando al atacante una interfaz para controlar el sistema comprometido. Un ejemplo de la GUI del cliente se muestra en la siguiente figura. Hay que notar como casi todas las opciones son el punto y haga clic. Todo atacante tiene que introducir la dirección IP de la víctima en la que ha instalado el troyano, conectarse a ese sistema, y el control de ese equipo. La barra de menú de la derecha le da al atacante una variedad de comandos para ejecutar en el equipo, de recuperación de contraseñas para el reinicio del sistema. Esta sencilla interfaz gráfica de usuario le dio a miles de atacantes la capacidad de controlar un sistema comprometido, lo que lo convierte en un arma muy popular.

Figura III.9. Interfaz de Back Orifice

Otro factor que hizo que Back Orifice una herramienta tan peligrosa era su flexibilidad. Adición de nuevas funciones o mejorar las capacidades fue muy fácil. En la tradición OpenSource, los programadores de todo el mundo mejoran el troyano. Por ejemplo, otros programadores pueden desarrollar plugins, llamados BUTTplugs, que amplían o mejoran la funcionalidad del Back Orifice. Una vez creados, estos complementos se distribuye rápidamente a través de Internet, permitiendo que cualquier persona en el mundo pueda descargarlo y utilizarlo.

Por ejemplo, el desafío con Back Orifice es conseguir que la víctima instale el troyano en su computador. Silk Rope fue un plugin diseñado para responder a este desafío. Silk Rope tiene un uso legítimo, como un dibujo animado. No hay manera de saber que ha sido infectado con excepción del aumento en el tamaño del ejecutable. La víctima recibe la caricatura animada infectada en el correo electrónico y lo ejecuta, no

darse cuenta de que ha sido infectado. Mientras que la caricatura se ejecuta y funciona como se esperaba, el troyano infecta el sistema de forma silenciosa. Para hacer el proceso aún más sencillo, un atacante podría falsificar el correo electrónico, haciendo que la víctima cree que proviene de una fuente de confianza, como un amigo. De esta manera un atacante podría simplemente enviar miles o incluso millones de correos electrónicos con archivos adjuntos infectados Back Orifice. Cada vez que una víctima inocente ejecute los archivos adjuntos, se convertirían en infectados. Todo atacante tiene que enviar miles de mensajes de correo electrónico y esperar a que los sistemas infectados respondan con sus direcciones IP. El atacante ya tenía el control total de un gran número de sistemas infectados.

Estas características flexibles y fáciles de usar alienta el uso generalizado del troyano. Miles de sistemas infectados, haciendo que el CERT organización de seguridad en Diciembre emitan una advertencia para evitar que el Back Orifice tenga un crecimiento generalizado. Desde que Back Orifice utiliza el puerto UDP predeterminado 31337 todo lo que uno tenía que hacer era escanear miles de sistemas de este puerto. Si este puerto se activa en un sistema, el sistema era muy probable que lo infecte, los atacantes podrían identificar los sistemas que ya están comprometidos.

3.3.2.1. El valor de BackOfficer Friendly

BOF es un honeypot de baja interacción Añade el valor a una organización principalmente mediante la detección y alerta a los ataques. Hay siete servicios preconfigurados en el que BOF puede detectar ataques. Cuando se realiza una conexión a cualquiera de estos siete servicios, el intento se registra y se genera una alerta.

BOF tiene cierta capacidad de emulación, pero es muy limitada. Ninguno de los servicios emula una aplicación específica o la versión, sólo la funcionalidad del

servicio. Por ejemplo, el servidor Web emula un servidor Web, que captura los intentos de obtener una página Web. Sin embargo, no emula un servidor web específico, como Apache o IIS. Esta funcionalidad limita a BOF principalmente a una tecnología de detección. Además, puesto que los servicios adicionales no se puede añadir o modificar, BOF se limita a la detección de ataques sólo en los siete puertos que BOF monitorea. Si el ataque se realiza contra cualquier otro puerto, BOF ignora de cualquier actividad maliciosa. Esto es una limitación común a la mayoría de los honeypots de baja interacción.

La prevención de ataques con BOF, por ejemplo, mediante el engaño o la disuasión, es difícil porque este equipo trampa ofrece poca interacción con el atacante. No se puede dar a un atacante información falsa, como banderas falsas o archivos falsos contraseñas etc, ya que BOF no tiene esa capacidad. También ofrece poco valor para la respuesta a incidentes. Aunque BOF detecta un ataque, le da poca información sobre lo que el atacante está haciendo, qué herramientas está utilizando, o cual es su intención. Una vez que BOF le avisa de las actividades de un atacante, otras tecnologías son necesarias para responder al ataque. Por último, BOF tiene muy poco valor como un sistema de este tipo, de nuevo debido a la poca información que obtiene. Una de las pocas implementaciones de investigación BOF tendría es el análisis de tendencias. Es decir, que podría ser utilizado para detectar los ataques en un período de tiempo. Esa información podría ser utilizada para construir un modelo estadístico de predicción de futuros ataques o las tendencias de exploración en el comportamiento, tales como un aumento repentino en la exploración de un servicio específico. Una vez más, esta capacidad es muy limitada, ya que se limitan a los siete servicios que ofrece HBO, y no se puede personalizar dichos servidores.

Cuando se detecta un ataque, la información capturada se limita a las transacciones de información, específicamente cuando ocurrió el ataque, la dirección IP de donde

venía el ataque, y que puerto fue atacado. Algunos de los servicios también puede determinar el tipo de ataque previsto. El propósito principal de la herramienta originalmente era capturar la actividad en el puerto por defecto UDP 31337.

BOF tiene otros seis servicios en los que puede escuchar en el que tienen el mayor valor, ya que estos son de uso general y ataque. En la Figura III.4 se muestra un ejemplo de detección de ataques BOF. En la alerta de BOF, vemos nueve conexiones diferentes capturadas en la naturaleza. Al tratarse de una trampa sin servicios de producción, las nueve conexiones son sospechosas.

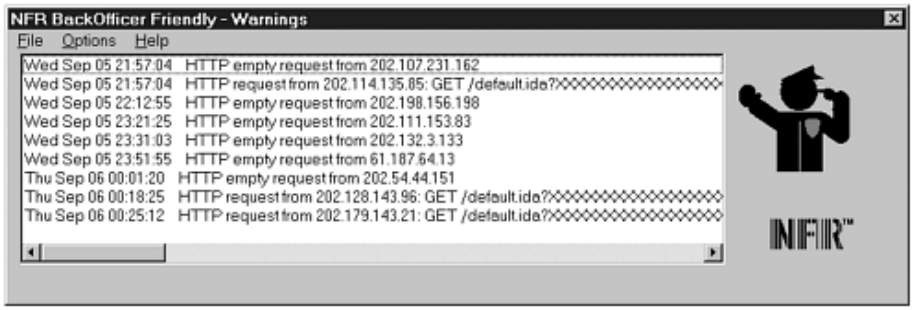

Figura III.10. Alertas de BackOfficer Friendly

Estos intentos de captura demuestran el valor principal de HBO, un recurso para detectar y advertir sobre la actividad maliciosa. En la figura anterior, se han detectado nueve posibles ataques en contra del equipo trampa en menos de cuatro horas. Tres de los ataques se confirman como los ataques CodeRed II. Si esta trampa se instaló en una red interna, esta información indicaría que hay debilidades en las defensas del perímetro, como un cortafuegos mal configurado, o que un sistema interno está infectado.

Al identificar estos riesgos, los problemas pueden ser fijos, tales como la corrección de errores en la base de reglas o de la identificación de los computadores internos infectados. Esto puede prevenir ataques posteriores. Los gusanos son cada vez más inteligentes en la selección de objetivos. CodeRed II demuestra que puedan empezar

de reproducción mediante el escaneo de sistemas en las redes locales en primer lugar. Esto significa que una vez que un gusano ha infectado a su red interna, es muy probable que se extendiera rápidamente. Un honeypot BOF podría usarse para detectar de forma rápida y alertar de la actividad del gusano.

Estas alertas también pueden tener otra ventaja: pueden demostrar a su dirección la necesidad de seguridad, el hecho de que las amenazas son reales. Muchas veces las organizaciones no se dan cuenta que son un objetivo, que los atacantes ven valor en sus sistemas y explotan sistemas vulnerables que puedan tener. Puede ser muy difícil para los administradores de seguridad para justificar la financiación nueva o de formación. Al demostrar que las amenazas a la gestión no existen, los administradores pueden ser capaces de obtener los recursos que necesitan. Los Honeypots pueden darle la munición para demostrar que las amenazas existen.

3.3.2.2. Cómo funciona BOF

Para que los puertos oyentes, seleccionen uno o más de siete servicios diferentes y escuchen en sus respectivos puertos y puedan capturar de cualquier conexión. Por ejemplo, tal vez al configurar un equipo trampa para controlar los cuatro servicios más comunes en la red interna, se selecciona el servicio FTP, el puerto 21, para monitorear las transferencias de archivos en contra de su intento de "honeypot". Selecciona el servicio SMTP, el puerto 25, para monitorear la actividad del correo. se está seleccionando HTTP, el puerto 80, para cualquier navegación por Internet. Por último, se selecciona POP3, puerto 110, para capturar a cualquier intento de transferencia de correo.

Si el sistema tiene el comando netstat-a, se puede identificar estos cuatro puertos abiertos. En la siguiente figura se da es un ejemplo del comando netstat-a que se

ejecuta en un sistema honeypot BOF, escuchando en los puertos 21, 25, 80 y 110. Los servicios creados por BOF se destacan. Cuando un atacante se conecta a cualquiera de estos cuatro puertos, BOF captará el intento y generar una alerta. Los otros puertos abiertos son puertos que figuran por defecto utilizado por el sistema operativo NT.

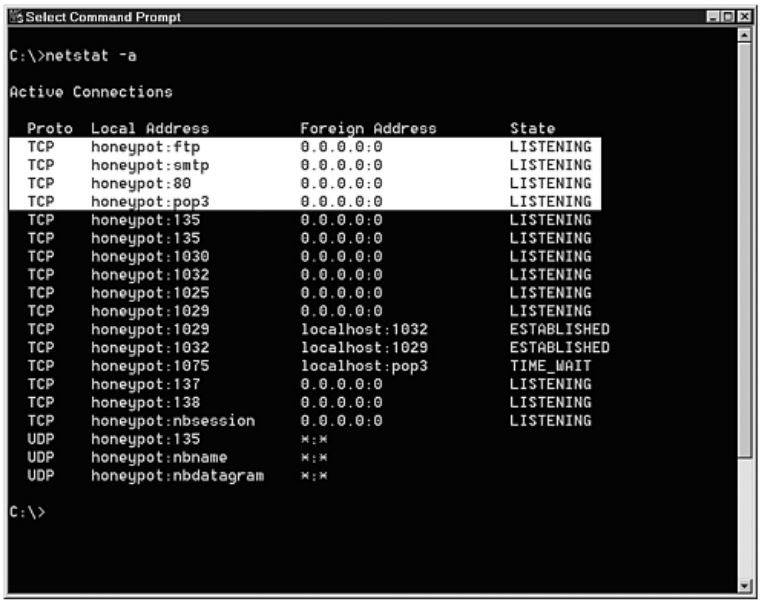

Figura III.11. Ejecución del comando netstat

Una cosa a considerar es que si se tiene cualquier otra aplicación que ya se está ejecutando en el sistema que tiene los puertos abiertos y escuchando. Si los puertos ya están registrados, a continuación, BOF no será capaz de monitorizar. Por ejemplo, si usted tiene un antivirus que se ejecutan en el escritorio, y el antivirus escucha en el puerto POP3 para escanear cualquier correo electrónico que recogen, a continuación, BOF no será capaz de escuchar en ese puerto y el monitor. Si ya dispone de un servidor Web o servidor FTP instalado en su equipo trampa, entonces BOF no será capaz de capturar cualquier actividad en cuestión. BOF sólo se puede escuchar en los puertos que ninguna otra aplicación está utilizando actualmente.

3.3.2.3. Instalación y configuración de BOF

BOF es uno de los honeypots que tienen las aplicaciones más sencillas y fáciles de Windows que se han instalado y configurado. Sólo hay que descargar el paquete en formato zip, descomprimir el archivo, y hacer doble clic en el icono BOF. Una vez que se haga doble clic en el icono bof.exe, el honeypot se encuentra instalado y funcionando. A continuación, se debe ver en su bandeja de menú en la esquina inferior derecha del sistema. El único paso que queda es configurar el honeypot.

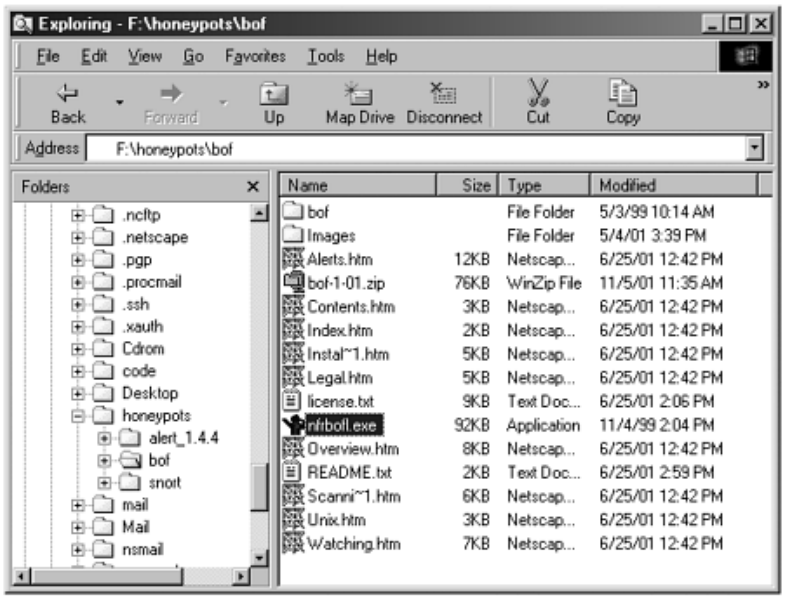

Figura III.12. Instalación de BOF

Hay que tener en cuenta que en realidad el programa es 92KB, muy pequeño y simple. El resto del material es la documentación basado en HTML, que es realmente muy bueno. Para configurar el equipo trampa, hace doble clic en el icono en la bandeja del usuario en la esquina inferior derecha. Se abrirá la consola BOF, como se puede ver en la Figura. Este menú sólo es de BOF. Todas sus configuraciones, mantenimiento, registros y alertas suceden con esta interfaz única, lo que hace BOF una solución sencilla de utilizar por cualquiera.

Lo siguiente que hay que configurar es el honeypot, para ello hay que plantearse algunas preguntas como: ¿Qué se quiere hacer? ¿Iniciar automáticamente el

honeypot? ¿Qué servicios desea que escuche? ¿Qué servicios se quiere emular? Según estas preguntas hay que configurar el equipo trampa utilizando el menú Opciones de la interfaz. Se le presentará con las opciones que se muestran en la siguiente figura.

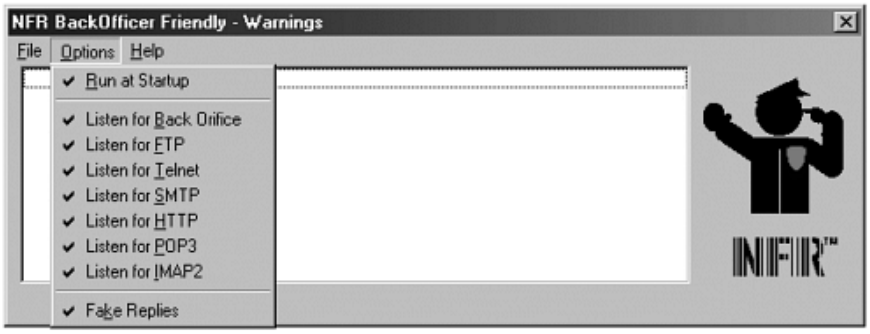

Figura III.13. Opciones BOF

La primera opción es ejecutar en el inicio. Es muy recomendable configurar BOF a partir del momento de que el sistema arranque. Hay que recuerdar, el honeypot no puede detectar ataques si no se está ejecutando. Hay que seleccionar los siete servicios, que son los que escucharán BOF y detectará los atentados en contra. No hay ninguna opción para crear sus propios servicios o los oyentes del puerto. Estos son los siete servicios que ofrece BOF:

Back Orifice

Es un troyano basado en Windows lanzado en 1998. Este servicio tiene un valor limitado, ya que este troyano no es de uso frecuente. Escucha en el puerto UDP 31337.FTP. Protocolo de transferencia de archivos. Un protocolo sin cifrar utiliza para transferir archivos. Escucha en el puerto 21 TCP. Este es un servicio muy común que los atacantes de destino. Lo más probable ver una gran actividad en

este puerto.Telnet. Un protocolo utilizado para cifrar por administrar de forma remota los sistemas. Escucha en el puerto TCP 23.

SMTP

Simple Mail Transfer Protocol. Un protocolo de texto sin formato utilizado para enviar y recibir correo electrónico. Escucha en el puerto TCP 25.

HTTP

Hyper-Text Transfer Protocol. Cleartext versión de la World Wide Web. Escucha en el puerto 80 TCP. De todos los servicios ofrecidos por HBO, este es el servicio más probabilidades de ser investigado o atacado. No hay ninguna opción o funcionalidad para escuchar el puerto TCP 443, conocido como Secure Socket Layer (SSL), puerto para conexiones cifradas Web.

POP3

Post-Oficina de Protocolo. Cleartext protocolo que utilizan los clientes para recuperar el correo electrónico. Escucha en el puerto 110 TCP.

IMAP

Internet Message Access Protocol. Cleartext protocolo que utilizan los clientes para recuperar el correo electrónico. Escucha en el puerto 143

TCP

Por último, se da la oportunidad de seleccionar la opción respuestas falsas, de forma predeterminada, sólo se escucha en el BOF los puertos seleccionados, y los registros de cualquier conexión. No tiene respuesta a emular a alguno de los servicios. Un atacante podría conectarse a uno de estos puertos, así que no hay ningún servicio prestado. BOF logra esto por haber concluido la conexión TCP y luego cerrar enviando un paquete RST, rasgando la conexión hacia abajo. En la figura 6.7, se ve un rastro de Snort de una conexión Telnet con un honeypot BOF (dirección IP 192.168.1.100) con falsas respuestas con discapacidad.

Sin embargo, si selecciona falso Respuestas, BOF permite a las capacidades de emulación. No sólo detecta las conexiones, sino también tratar de responder a ellas. BOF emula los servicios y las aplicaciones responden como lo haría, pero esta capacidad de respuesta es muy limitada. Por ejemplo, con la emulación de Telnet, el atacante sólo puede tratar de darle un nombre de usuario y contraseña. No hay banners para emular sistemas operativos específicos o cualquier respuesta específica que puede seleccionar. El servicio HTTP no emula cualquier tipo específico de servidor Web, sino que sólo capta el comando enviado por el atacante. La ventaja de las falsas respuestas es que la información se puede obtener más. La desventaja es que el atacante más probable es que sabe que su actividad ha sido registrada. Él lo sabe porque al interactuar con la aplicación, algún tipo de registro tiene que haber ocurrido.

Una vez que seleccione las opciones en el menú Opciones, inmediatamente en vigor. No hay reiniciar o cualquier reanudación de los servicios o los motores de emulación. BOF es extremadamente sencillo: Seleccione lo que desea, y sucede inmediatamente.

Una vez que HBO está instalado, usted está listo para ir. No hay parches o actualizaciones han sido puestos en libertad desde 1998, por lo que muy probablemente no tienen que preocuparse de actualizar los honeypots. Una desventaja de BOF es que no hay capacidad para administrar de forma remota honeypots BOF. Una vez instalada e implementada, toda la gestión y configuración debe ocurrir a nivel local en el sistema. Como tal, esta no es una solución empresarial. BOF no fue diseñado para ser desplegado a lo largo de una gran corporación. No existe un mecanismo centralizado para la configuración y mantenimiento. En cambio, todo tiene que ocurrir en el sistema al que está instalado localmente. Su uso principal es como un honeypot de escritorio que se

ejecutan en sistemas individuales, tales como los sistemas de seguridad o los administradores de red.

3.3.2.4. Recopilación de Información y Alerta de Capacidades

Como hemos discutido, las capacidades de HBO sobre acopio de información son limitadas. Se puede controlar sólo siete servicios. La información recogida para los siete servicios se limita a la fecha y la hora del ataque, la dirección IP del sistema de ataque, y el puerto lo atacaron. Si la opción de Fake Respuestas está habilitado, entonces los servicios serán emulados, dando al atacante algo para interactuar con. Información adicional puede ser obtenida, como el login y la contraseña que se utiliza en el servicio Telnet o de la solicitud GET para el servicio HTTP. Sin embargo, esta interacción es muy limitada y dependiente del servicio específico.

Cuando detecta una conexión BOF, se genera una alerta, y la interfaz de BOF aparece en la pantalla de los sistemas. La Figura III.8. ilustra este proceso de alerta. Sin embargo, este es el único mecanismo de alerta BOF apoya. No tiene capacidad para registrar información de forma remota, ni puede generar una alerta y enviarlo por correo electrónico o página de un administrador. No tiene capacidades remotas de alerta. Alerta es hecho visualmente advertencia de que un ataque se ha producido. Si se genera una alerta en una noche de viernes, el administrador del sistema lo más probable es ser consciente de ello hasta que regrese al sistema de la mañana del lunes. Así como no hay manera de administrar de forma remota un equipo trampa BOF, no hay manera de alertar de forma remota. Esto hace que sea una opción muy pobre para implementaciones empresariales. Gestión de las alertas de múltiples honeypots BOF sería demasiado larga.

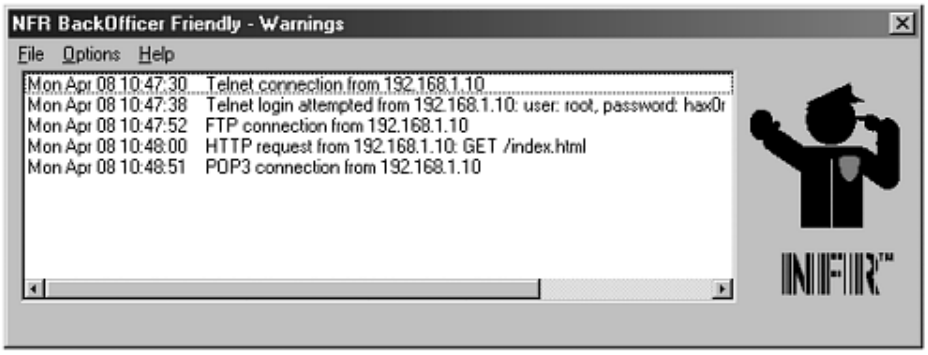

Figura III.14. Proceso de alerta de BOF

En la figura III.14. Vemos un ejemplo de varias conexiones hechas a la honeypot, en este caso un honeypot BOF con Fake Respuestas habilitado. En las dos primeras detecciones, vemos un intento de Telnet a partir de la fuente 192.168.1.10. La primera alerta por Telnet nos advierte que alguien se ha conectado al servicio Telnet emulado. La segunda alerta por Telnet nos dice que el atacante trató de entrada, utilizando la cuenta de root y la contraseña hax0r. Potencialmente, el atacante está buscando puertas traseras en los sistemas conocidos troyanos. Después, el atacante intentará realizar una conexión FTP, pero BOF emula un servidor FTP con discapacidad. Después de la conexión FTP, vemos que el atacante realiza una conexión con su navegador e intenta obtener la página Web principal, index.html. Esto puede ser una sonda para determinar qué tipo de servidor Web que se están ejecutando. A raíz de la petición HTTP registra, vemos una conexión final al emulado servicio POP. Esto demuestra la extensión y limitaciones, de las capacidades de HBO sobre acopio de información.

Una característica agradable de BOF se puede volcar toda la actividad registra en un archivo de texto ASCII, lo que hace la información mucho más fácil de leer. La información puede ser descargada en una base de datos o revisada por los guiones para obtener información adicional, tales como análisis de tendencias. Para volcar las

alertas a un archivo de texto ASCII, simplemente entrar en el menú, en Archivos y luego seleccione guardar las descripciones. A continuación se le pedirá que dé el nuevo archivo un nombre y guardar los archivos.

Esta capacidad es crítica, ya que el menú BOF se puede convertir rápidamente abrumado con las descripciones, por lo que es extremadamente difícil para revisar toda la actividad registrada. Por ejemplo, la Figura III.9. es una captura de pantalla de BOF online de mi red doméstica personal durante cuatro días. El honeypot fue atacado varias veces, principalmente por los gusanos en busca de servidores Web de IIS vulnerables. Todos estos ataques pueden desbordar rápidamente la interfaz de BOF. La pantalla muestra lo difícil que puede ser el examen de las alertas que se reunieron con el tiempo. Pero con la capacidad de BOF para salvar a la información registrada en un archivo de texto ASCII, esta información puede ser manejada eficientemente.

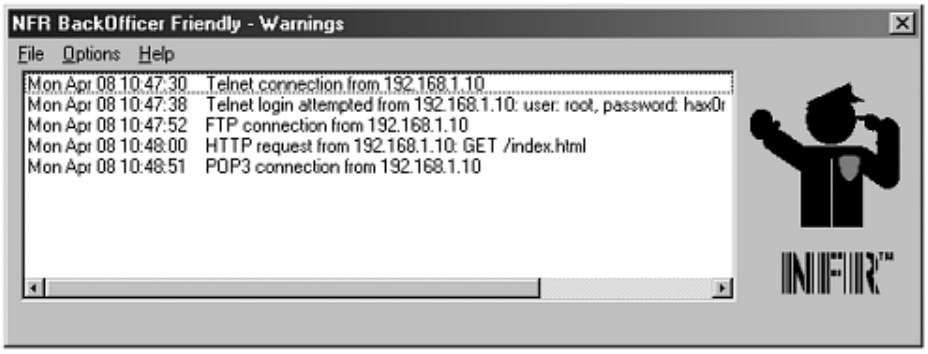

Figura III.15. Captura de pantalla BOF

3.3.2.5. Riesgo asociado a BOF

Como un honeypot de baja interacción, BOF añade muy poco riesgo. Realmente no hay nada para el atacante de interactuar con o explotar. En el momento de escribir esto, no se conocen exploits para la aplicación. La aplicación real es muy pequeño en tamaño-98 Kbytes-lo que significa que es muy poco código en cuestión. Como tal, esto limita el potencial de vulnerabilidades. El riesgo radica en el sistema en el que está

instalado BOF. Debe asegurarse de que el sistema se está asegurada. Un atacante no puede ser capaz de explotar cualquier servicio en BOF, pero puede ser capaz de explotar cualquier explotación de Windows que existe en el propio sistema. Como tal, las mejores prácticas deben aplicarse al sistema operativo base.

Sin embargo, BOF tiene un alto riesgo de detección si se utiliza falsas Respuestas. Al interactuar con los servicios de BOF emulado predefinidos, puede ser muy fácil determinar la identidad de BOF. BOF no tiene las características de personalización, emulación es activada o desactivada. Es relativamente fácil para un atacante para descargar e instalar en su BOF propios sistemas. Desde allí se puede estudiar la solución honeypot y aprender cómo funciona. El desarrollo de las impresiones dactilares para el honeypot no sería difícil. Basándose en estas huellas dactilares, los atacantes podrían identificar las implementaciones de BOF. Es difícil contrarrestar ese riesgo si está utilizando falsas respuestas, ya que no puede modificar las implementaciones de BOF. Se podría añadir servicios adicionales a los sistemas con BOF instalado, como oyentes puerto, como se discutió en el capítulo 9. Sin embargo, si empezar a poner más trabajo en cada implementación honeypot BOF para mitigar el riesgo de detección, entonces tal vez usted debería considerar otras alternativas honeypot. Si usted está preocupado por las huellas dactilares, entonces lo más probable es que desee deshabilitar la funcionalidad falso respuestas, escuchar.

3.3.3. SPECTER

Al igual que BOF, Specter es un honeypot de baja interacción emula una variedad de servicios. Es el siguiente honeypot lógico para examinar, porque introduce una variedad de características y funcionalidades. Estas características adicionales amplian las capacidades de los honeypots en la detección, alerta y recogida de información. A diferencia de BOF, Specter es un honeypot diseñado para el entorno empresarial.

3.3.3.1. Listado de Specter

Specter es un honeypot mercantil creado y apoyado por NetSec, una empresa de seguridad de red con sede en Suiza. Conceptualmente es similar a BOF en el que los atacantes no tienen un acceso al sistema operativo. Una solución de software se instala en un sistema y emula una gran variedad de atacantes que pueden interactuar con los servicios. Los atacantes se limitan a lo que la funcionalidad del software que proporciona Specter.

Specter es más intensivo en recursos que BOF, y sólo puede funcionar en algunos sistemas Windows. Desde la versión 6.0, sólo se puede ejecutar en Windows NT Service Pack 6a, 2000 SP1 y XP. También requiere al menos un procesador Pentium II de 450 MHz y 128 MB de RAM. Debido a estos requisitos, lo más probable es que desee sistemas dedicados para honeypots Specter.

A pesar de Specter es conceptualmente similar al BOF, Specter tiene capacidades mucho mayores. Estas capacidades mejoradas lo distinguen como una solución empresarial. La primera gran diferencia está en el número de servicios que puede controlar. Specter viene con siete servicios emulados completamente, seis trampas, y una trampa personalizable. Esta flexibilidad le da el poder para detectar los ataques a 13 puertos predefinidos y 1 puerto configurable. Al hacer referencia a una gama más amplia de puertos, Specter puede detectar un mayor número de ataques diferentes.

Una segunda diferencia es en la capacidad de Specter para emular las aplicaciones. Esta emulación es similar a la de las respuestas falsas, habilitadas en BOF, donde los servicios de imitar a la interacción de las aplicaciones reales. Sin embargo, los servicios emulados de Specter tiene un mayor realismo y la interacción integrada en ellos, así que parece mucho más auténtica a la atacante. Por ejemplo, cuando Telnet para un honeypot BOF, sólo tiene que conseguir una entrada del sistema. Sin

embargo, cuando Telnet para un honeypot Specter, usted consigue una bandera indicando entrada depende del sistema operativo de información, tal vez algunos mensajes de error, y luego una entrada interactiva del sistema. Con BOF, el servidor Web emulado sólo escucha en el puerto 80 y registra cualquier intento de conexión. Specter tiene este nivel de interacción más allá al proporcionar un verdadero servidor Web con las páginas Web que un atacante puede interactuar. Usted puede incluso modificar las páginas Web, añadiendo sus propios contenidos y gráficos, creando así un "honeypot" más realista.

Una característica única de estos servicios es que tienen la capacidad de emular no sólo la interacción, sino también vulnerabilidades. Un blackhat puede lanzar un ataque contra un servicio de Specter y cree que el ataque fue un éxito cuando en realidad no lo era. Specter puede retroalimentar información falsa al atacante, confundirlos o al menos perder el tiempo. Por ejemplo, uno de los siete servicios que emula Specter es FTP. Si Specter ha sido configurado para actuar como un servidor FTP vulnerable, los intrusos pueden caer en la trampa y ejecutar una variedad de comandos. Un uso de una táctica común es que muchos atacantes se están descargando el archivo del sistema comprometido. Este archivo se utiliza para obtener más información sobre las cuentas de usuario y, a veces incluso las contraseñas de usuario. Specter emula esta vulnerabilidad, incluso, ofrece al atacante un archivo real con contraseña falsa con la que el atacante puede intentar analizar y tal vez incluso crackear. Esta vulnerabilidad emulada interactúa con el atacante, proporcionando las respuestas a un intruso que espera de un servicio vulnerable. El atacante realiza con éxito las descargas de un archivo de contraseñas que es en realidad un archivo falso.

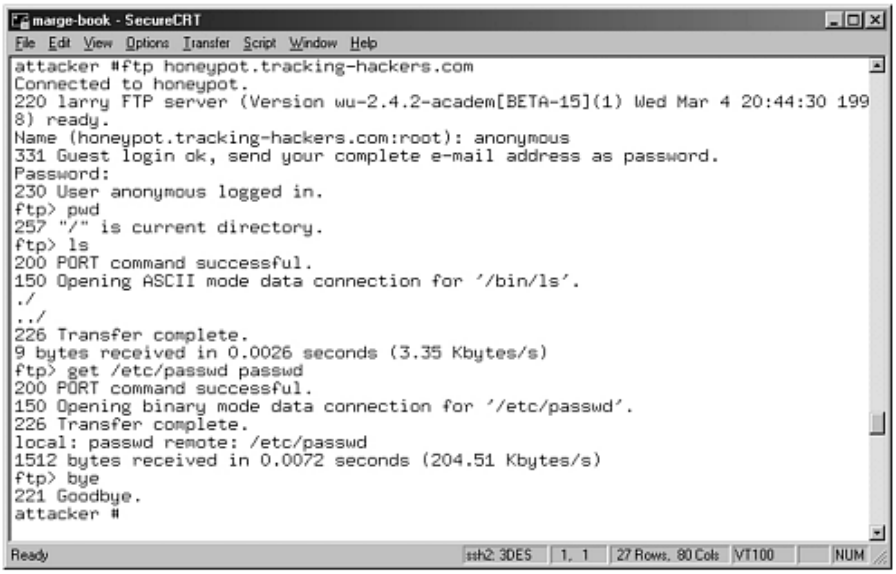

Figura III.16. Captura de ataque a Spectec

Además de los siete servicios predefinidos, Specter tiene lo que llama las trampas. Las trampas no emulan los servicios, pero escuchan los puertos previamente designados, detecta y registra todas las conexiones. Esto es similar a cuando BOF falso Respuestas está deshabilitada. El atacante no interactúa con el puerto o servicio, el intento de conexión se registran en silencio por el honeypot. Specter viene con seis trampas predefinidas y una trampa personalizable, lo que le permite designar a un puerto en el que escuchar y detectar cualquier actividad. Esta trampa personalizable es extremadamente útil, lo que le permite adaptar el equipo trampa a las nuevas amenazas o vulnerabilidades. Por ejemplo, tal vez una nueva vulnerabilidad ha sido identificada para MySQL, por lo que están preocupados por la exploración en el puerto TCP 3306. O tal vez un nuevo troyano ha sido puesto en libertad, y usted quiere detectar las sondas para el puerto por defecto administrativo. Como sabemos las amenazas están siempre adaptándose y cambiando, y así va a honeypots. La trampa configurable permite modificar su trampa como amenazas continúan cambiando.

Además de emular a los distintos servicios, Specter tiene la capacidad de emular 13 sistemas operativos diferentes, un sistema operativo a la vez. Esta capacidad le da la flexibilidad para determinar cómo se aplican las amenazas a los sistemas operativos diferentes. La mayoría de las organizaciones a implementar una variedad de sistemas operativos diferentes, por lo que Specter se puede adaptar fácilmente y se funden en los diferentes ambientes.

Otra característica única de Specter es la posibilidad de personalizar el honeypot. Cada instalación de BackOfficer Friendly tiene el mismo aspecto. No hay manera de alterar la identidad de la trampa. Esto no sólo previsibilidad crear un honeypot menos realista, pero que potencialmente puede ser una firma. Cada trampa BOF se comporta exactamente de la misma, por lo que es más fácil para los atacantes para detectar de forma remota. Sin embargo, con Specter, una variedad de modificaciones se pueden hacer, dando a la trampa de su propia identidad o personalidad. Esto ayuda a crear un honeypot más realista y menos identificable.

Puede asignar el honeypot Specter su propio nombre, dirección de dominio, o un mensaje de advertencia personalizado. Incluso puede asignar Specter su propia personalidad, lo que el sistema de características específicas. Specter tiene cinco personajes predefinidos que puede asignar, cada uno con su propia identidad. Cada una de estas cinco características hará el acto trampa de una manera única. Todas estas características le permiten personalizar el honeypot que mejor se adapte a su entorno.

3.3.3.2. El valor de Specter

Specter es una solución altamente flexible, apoyando una variedad de funciones. Como resultado, puede desempeñar diversas funciones para una organización. Al igual que BOF, Specter es una excelente herramienta para la detección de ataques o actividades no autorizadas. De hecho, este es uno de sus principales funciones: la

función como una tecnología de detección de intrusos. Sin embargo, debido a sus numerosas opciones, Specter también se puede utilizar en el campo de engaño o la disuasión, la prevención de posibles ataques. Puede ser diseñado para dar una gran cantidad de información falsa a un atacante, confusa o engañosa ella. También puede ser utilizado para ahuyentar a los atacantes, disuadirlos de nuevos ataques.

Sin embargo, Specter está limitada en el tipo de información que puede recopilar, similar a la HBO. Como tal, proporciona un valor poco en reaccionar a un incidente. Se puede detectar cuando un ataque ha ocurrido y la fuente de los ataques, pero no puede capturar los detalles de las actividades de los atacantes, como sus herramientas o cargas de paquetes. Estas limitaciones también reducen su valor como un sistema de este tipo. Puede ser utilizado para el análisis de tendencias o modelos estadísticos de tipos y la frecuencia de los ataques, pero no puede capturar la información necesaria para la mayoría de las actividades de investigación. Como tal, el valor de Specter se encuentra principalmente en la detección de ataques, con un valor secundario en la prevención de ataques.

Para fines de detección, Specter opera de manera similar a BOF. Cuenta con hasta 14 puertos en los que se escucha. Las conexiones a los puertos se detectan y registran, a continuación, se genera una alerta. Desde el honeypot no tiene tráfico producción esperada, todas las conexiones se supone que son hostiles. Acciones Specter dos ventajas significativas sobre BOF para detectar ataques. La primera es que Specter tiene el doble de la cantidad de puertos que puede controlar. Esto significa que potencialmente el doble de la cantidad de ataques diferentes pueden ser detectados. Además, uno de estos puertos es personalizable, lo que el honeypot la flexibilidad para adaptarse y detectar nuevas amenazas. Sin embargo, aún más importante es la opciones eficaces de alerta Specter. Son estas opciones de alerta que hacen Specter como una tecnología de detección de gran alcance.

Cuando BOF detecta un ataque, que aparece en la consola, notificando al administrador del sistema del ataque. Este mecanismo de alerta es muy limitado. El administrador debe tener acceso físico al sistema y revisar la interfaz gráfica de usuario para ser notificado de la actividad detectada. Esto repercute negativamente en el valor de un honeypot. ¿De qué sirve un honeypot cuando detecta algo, pero nadie está a saberlo? BOF puede detectar una actividad de ataque en una noche de viernes, pero el administrador de seguridad no saber de él hasta que tres días más tarde- cuando ella viene en la mañana del lunes. Para entonces el ataque detectado ha perdido su valor, el atacante ha tenido tiempo amplio para actuar.

Specter resuelve este problema mediante el apoyo a diferentes formas de alertar a las personas de forma remota a la actividad detectada. Estas opciones son altamente personalizables, dando a los administradores de varias maneras para recibir una alerta en tiempo casi real. El personal de seguridad no necesita acceso físico al sistema para recibir una alerta para los atacantes. Los métodos incluyen detalladas alertas de correo electrónico, alertas de correo electrónico corto diseñado para localizadores y mensajes de syslog para el registro remoto. Estas capacidades proporcionan a los administradores de alerta de seguridad de la información que necesitan de forma rápida y en un valor de formato fácil de usar, incrementando en gran medida la detección y alerta de Specter.

El engaño y la disuasión son un segundo y único lugar, el valor de Specter. Como ya comentamos anteriormente los honeypots pueden ser potencialmente utilizados para prevenir los ataques. Esto se hace en una de varias maneras. El primero es el engaño: para confundir o desorientar a un atacante. El honeypot puede alimentar la información atacante falsos, por lo que es mucho más difícil y requerir mucho tiempo para ellos para atacar a los recursos. Una segunda posibilidad es la disuasión. Honeypots pueden potencialmente ser utilizado para ahuyentar a los atacantes, ya sea por advirtiéndoles o simplemente con su presencia. Si los atacantes de conocer una

organización está utilizando honeypots, que ni siquiera intento de ataque porque no pueden distinguir un objetivo válido de una trampa. Sin embargo, como lo hemos indicado, el engaño y la disuasión son armas psicológicas, y, como tales, sólo funcionan contra las personas. Si su organización está siendo investigado o atacados por las herramientas automatizadas, como los gusanos o hinchas de automóviles, estos mecanismos de defensa se hacen poco para prevenir los ataques.

Specter puede engañar a un atacante en una de varias maneras. En primer lugar, se puede alimentar a un atacante la mala información. Por ejemplo, las páginas Web se pueden crear para emular una organización. La información falsa puede ser publicada en el sitio Web, tales como nombres falsos, cuentas o documentación falsa. Specter también tiene la capacidad para distribuir archivos falsos contraseña. Los atacantes creen que han capturado los datos clave de gran valor cuando en vez que han sido engañados en la recuperación de los inicios de sesión falsificados. Specter también puede confundir a los atacantes y perder el tiempo dando una respuesta extraña o actuando de manera extraña. Marco de la personalidad que el honeypot de causas extrañas que se comporte de una manera inesperada.

Otro mecanismo es la vulnerabilidad emulado. Blackhats podría lanzar un exploit que Specter simula el mismo éxito. El atacante sigue con el ataque, esperando el acceso al servicio emulado, pero esto es acceder a la trampa nunca permitirá. A medida que el atacante sigue intentando acceder, debido a su éxito inicial, que se confunde y sólo los desechos de más tiempo. Esta vez ofrece a las organizaciones una mejor oportunidad de responder de manera eficaz.

Specter también pueden disuadir a los atacantes, en particular cuando su carácter es agresivo. Al dar curso agresivo, Specter tratará de alertar y asustar a los atacantes si siente que está siendo atacado. Por ejemplo, Specter puede determinar que un atacante pone en marcha una web común explotar en contra de su aplicación de servidor Web. Una vez que ha captado toda la información sobre el atacante, Specter

le advertirá al intruso que sus acciones se han detectado, todos los de su actividad y la identidad se ha registrado, y que los administradores están respondiendo al ataque. Por lo general, esta información asusta a la atacante.

Tenga en cuenta que la disuasión y el engaño puede ser difícil de establecer y aplicar, tomando los recursos críticos que puede ser usado para asegurar los sistemas de producción. Specter contadores de esto por lo que es fácil de implementar estas capacidades. Si bien el engaño y la disuasión son fáciles de implementar con Specter, sigo considerando que el valor de detección primaria de Specter.

Lo más emocionante es cómo Specter ha combinado todas estas características en un muy fácil de formato de uso. Como veremos en capítulos posteriores, hay honeypots que tienen una mayor flexibilidad y funcionalidad que Specter pero estos honeypots requieren mucho más tiempo y recursos para configurar y mantener. Por lo tanto, muchas organizaciones no pueden usar los honeypots más sofisticado, o el tiempo invertido en ellas no puede valer la pena el regreso. Specter, como veremos, es muy fácil de configurar y mantener. La simplicidad de esta trampa en sí mismo lo hace valioso. La más sencilla sea la solución, la menos probable es que se cometen errores aplicación.

3.3.3.3. Cómo funciona Specter

Al igual que BOF, Specter se escucha en los puertos respectivos para cualquiera de los servicios o las trampas que ha seleccionado. Si su sistema tiene el comando netstat-a, mostrará los puertos que ha seleccionado y habilitado como abiertos y escuchando. Specter comparte las mismas limitaciones que BOF. En concreto, no se puede escuchar en un puerto o un monitor que ya es propiedad de otra aplicación. Si tiene algún servicio de escucha en el puerto FTP (puerto 21), a continuación, Specter no puede controlar en ese puerto. Si está ejecutando su propio servidor Web personal

en la trampa, a continuación, Specter no puede controlar el puerto 80. Specter sólo puede controlar los puertos que no son propiedad de ninguna otra aplicación.

Como mencionamos anteriormente, Specter también tiene la capacidad de emular diferentes sistemas operativos. Esto se hace cambiando el comportamiento de los servicios de imitar el sistema operativo seleccionado. Por ejemplo, si se selecciona el honeypot para funcionar como un servidor Windows XP, los servicios emulados se comportan como un sistema Windows XP. Cuando se conecta al puerto 80, el servidor Web, usted estará rodeado por un IIS (Internet Information Server) la página del servidor Web, exactamente igual que lo se esperaría encontrar en un nuevo servidor de Windows XP. Las trampas no alteran su comportamiento basado en el SO seleccionado, ya que no emulan servicios específicos. Sólo vigilan los puertos de la actividad. Todos los sistemas operativos emulados se realizan por los siete servicios.

Si selecciona el sistema operativo Solaris a continuación, los siete servicios emulados se comportaran como un servidor Solaris. Por ejemplo, cuando se conecta al puerto del servidor Web, se consigue una página Web diferente. En la mayoría de los casos, de servidores web Solaris no se ejecutan aplicaciones de Microsoft, como el servidor Web de IIS. En su lugar, se ejecutan los diferentes tipos de servidores Web, como Apache o un servidor Web iPlanet. Así. En el caso de Solaris, el servidor emulado Web actúa como un nuevo servidor web Apache, una de las aplicaciones más usadas Web para sistemas Unix.

Los siete sistemas emulados participan de servicios de inteligencia similares, teniendo la capacidad de actuar como el sistema operativo seleccionado. Si se configura el equipo trampa en un sistema Linux, cada vez que un atacante telnet se conecte, se recibirá un mensaje de login de Linux. Si se selecciona el sistema operativo MacOS cuando ingrese un atacante FTP, se recibirá una bandera MacOS entrada FTP.

Otro ejemplo de emulación de aplicación es el uso de contraseñas. Specter tiene un conjunto de contraseñas falsas que están disponibles para "capturar" a los atacantes.

El archivo de contraseñas es realmente una planta, situada en la trampa de ser tomado deliberadamente por el atacante. El sistema operativo que seleccione determinará qué tipo de atacantes contraseña puede capturar. Si el honeypot es un sistema basado en Windows, como Microsoft 2000, a continuación, la base de datos de las contraseñas capturadas serán en formato de Windows. Si configura Specter para emular un sistema operativo basado en Unix, como Solaris o Linux, a continuación, la base de datos contraseña será en formato Unix. Una vez más, Specter tiene la inteligencia en el nivel de aplicación para responder como el sistema operativo correctamente configurado.

Desafortunadamente, cuando emula un sistema operativo, Specter sólo opera a nivel de aplicación. Esto significa que sólo emula el sistema operativo elegido sobre la base de los siete servicios emulados. A pesar de que su equipo trampa y la trampa son los servicios de emulación de un servidor Linux o MacOS, la IP sigue siendo de Microsoft.

Esto significa que todas las comunicaciones basadas en IP y de la utilización honeypot IP del sistema operativo. Specter en la actualidad sólo se ejecuta en sistemas basados en Windows, por lo que siempre se utiliza el IP de Windows. Cada sistema operativo tiene sus propias características únicas que se pueden utilizar para identificar positivamente el sistema.

Fiodor, un programador de seguridad altamente calificado, ha desarrollado la herramienta de escaneo en red de Nmap. Como una herramienta de escaneo de puertos, Nmap remotamente puede determinar cuáles son los servicios de un sistema

que están en funcionamiento. Esto es usado por muchos administradores de sistemas para identificar vulnerabilidades en su red. Nmap también tiene la capacidad para determinar activamente el tipo de sistema operativo de un sistema remoto. La respuesta del sistema remoto de estos paquetes es capturado y registrado. Esta información se registra a continuación, en comparación con una base de datos de firmas del sistema operativo, una base de datos que ha grabado la mayoría de los tipos conocidos de sistemas operativos y como se comportan. Con base en estas firmas, se puede determinar el tipo de un sistema operativo.

3.3.3.4. Instalación y configuración de SPECTER

Como la mayoría de aplicaciones basadas en Windows, la instalación es muy simple. Descargar el paquete comprimido, descomprimirlo, y luego hacer doble clic en el icono de instalación. Specter a continuación le llevará a través de varias pantallas, ya que instala el equipo trampa. El proceso de instalación es el procedimiento estándar de instalación de Windows. Una vez completo, tarda treinta segundos y ya está listo para poner en marcha la trampa y configurarlo.

La configuración de Specter es similar a HBO pues es simple y fácil de usar la interfaz gráfica llamada Specter Control para configurar el equipo trampa. Sólo hay una interfaz gráfica de usuario todo está en la pantalla al mismo tiempo para la instalación y la configuración de la toma de la creación de la trampa es muy fácil. La interfaz gráfica de usuario tiene las categorías de configuración con las opciones en cada categoría. Sólo se tiene que activar la opción de elección haciendo clic en el botón correspondiente. Para obtener ayuda en cualquiera de los temas, basta con hacer clic sobre la cuestión botón junto a cada opción.

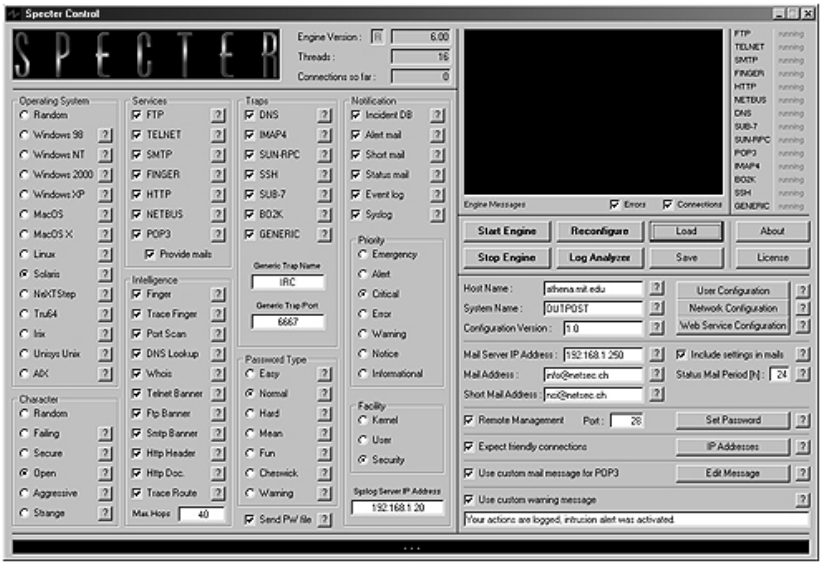

Figura III.17. Interfaz de Specter

TELNET sirve una amplia variedad de propósitos. A menudo se utiliza para establecer conexiones de los terminales con equipos remotos. El servidor TELNET es muy probable que sea examinado por un atacante.

En las secciones siguientes se explica cada una de las opciones de personalización.

3.3.3.4.1. Sistema Operativo

Al empezar a configurar el equipo trampa en la columna de la izquierda se selecciona qué sistema operativo se desea emular. Como se señaló anteriormente, el sistema operativo que seleccione afectará a cómo se comportan los servicios. Si no puede decidir cuál de los 13 sistemas operativos va a emular, siempre se puede seleccionar al azar. Al seleccionar un tipo de sistema operativo, modifica el comportamiento de los siete servicios emulados. Los 13 sistemas operativos, desde la Versión 6.0, son los siguientes:

- Windows 98
- Windows NT

- Windows 2000
- Windows XP
- Linux
- Solaris
- Tru64 (formerly Digital Unix)
- NeXTStep
- Irix
- Unisys Unix
- AIX
- MacOS
- MacOS X

3.3.3.4.2. Personaje

El siguiente paso es determinar cómo quiere que su equipo trampa de comportarse, su personalidad. Usted tiene una de las cinco personalidades para elegir: A falta de, seguro, abierto, agresivo, y extraño. Cada una de estas características afecta directamente a cómo los servicios emulados se comportarán. Así como los sistemas operativos seleccionados afectan al comportamiento de los servicios de replicar sistemas específicos, la característica seleccionada afecta al comportamiento de los servicios para replicar un sistema de personalidad.

Por ejemplo, Open crea un sistema que tiene una variedad de servicios de fácil acceso, similares a las instalaciones por defecto muchos de un sistema. Si un atacante para conectar al puerto SMTP y validar si la trampa tiene la capacidad de retransmisión de correo, el honeypot simula que la vulnerabilidad existe. Muchos atacantes o herramientas automatizadas hacen esto para determinar si un sistema se

puede utilizar para transmitir de forma anónima por correo, más a menudo de los ataques de spam. La siguiente figura muestra un ejemplo de un honeypot Specter se prepara para abrir y correo habilitado relé. Un atacante tendría que este sistema es vulnerable.

Si la trampa está en seguro, el honeypot que emula la funcionalidad del relé ha sido desactivado. Sobre la base del ejemplo de retransmisión de correo, el honeypot responde que el servicio ha sido desactivado, ya que cualquier sistema seguro debe responder.

Como es agresivo, la personalidad trampa está diseñada para ahuyentar a los atacantes. Cuando Specter determina que el atacante está tratando de actividad no autorizada, el honeypot se identificará como un dispositivo de detección de intrusos y alertar al atacante que se han detectado y registrado. Por ejemplo, si un atacante se conecta al puerto SMTP y trata de confirmar si la retransmisión de correo es vulnerable, el honeypot interpretaría esto como una actividad no autorizada. Se podría bloquear el intento e informar al usuario atacante que sus intentos han sido detectados. Figura III.18 muestra la misma consulta para la retransmisión de correo.

Sin embargo, dado el carácter de este equipo trampa se establece en agresivo, que no imita un sistema vulnerable. En cambio, cuando se determina relé verdadera intención del atacante-mail-que bloquea los intentos del atacante y le advierte que fuera.

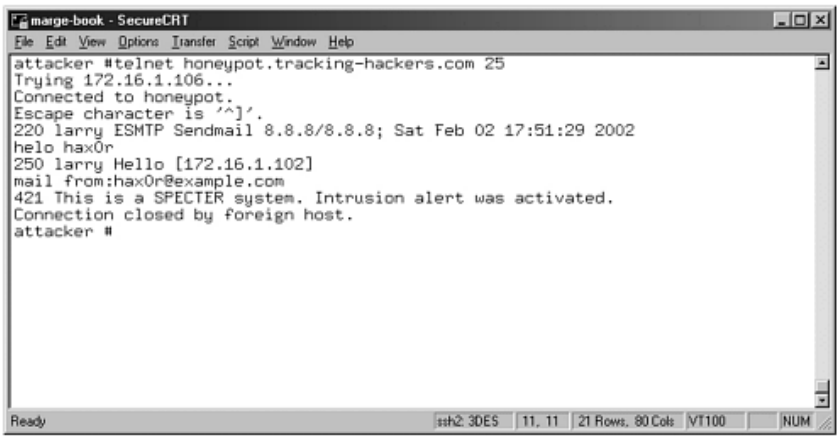

Figura III.18. Consulta para la retransmisión de correo

A falta de actos como los servicios que se han configurado correctamente o tiene errores. Un atacante podría conectar al puerto SMTP y de retransmisión de correo intento, y el honeypot, simplemente contestaba con errores solicite el servicio no era posible. Extraño está diseñado para confundir a un atacante, actuando como un fracaso o extrañamente configurado el sistema. En el caso de SMTP, que actúa como un sistema abierto. Sin embargo, los actos de servidor Web como un sistema mal configurado, la información de un método 501 No implementado error.

Estas características opcionales le dan la oportunidad de crear un honeypot más dinámica y flexible, dependiendo de lo que están tratando de lograr. Por último, no al azar como su nombre implica: selecciona al azar una característica cada vez que alguien se conecta a la trampa. Esta es una excelente opción para personas que no pueden decidirse. Al azar ayuda a ocultar la identidad de la trampa de los atacantes, ya que no existe un patrón de comportamiento que pueden ser fácilmente sus huellas digitales.

3.3.3.4.3. Servicios

El siguiente paso es seleccionar cuál de los siete servicios que desea activar. Estas son las aplicaciones reales emulado. En cuanto a la versión 6.0, los siete servicios emulados son:

- **FTP** File Transfer Protocol. Un protocolo de texto plano utilizado para transferir archivos. Escucha en el puerto TCP 21. Este es un servicio muy comunes los atacantes de destino. Lo más probable ver una gran actividad en este puerto.
- **Telnet** Un protocolo sin cifrar para administrar de forma remota los sistemas. Escucha en el puerto TCP 23.
- **SMTP.** Simple Mail Transfer Protocol. Un protocolo de texto plano utilizado para enviar y recibir correo electrónico. Escucha en el puerto TCP 25.
- **FINGER** Se utiliza para obtener información sobre los usuarios en sistemas remotos. Escucha en el puerto TCP 79.
- **HTTP** Hyper-Text Transfer Protocol. Sin cifrar por la versión de la World Wide Web. Escucha en el puerto TCP 80. De todos los servicios ofrecidos por Specter, este es el servicio más probabilidades de ser investigado o atacado. No hay ninguna opción o funcionalidad para escuchar en el puerto 443, conocido como Secure Socket Layer (SSL), para conexiones cifradas Web.
- **NetBus Windows Troya**. Escucha en el puerto TCP 12345.
- **Protocolo POP3 Post-Office**. Protocolo de texto no cifrado que utilizan los clientes para recuperar el correo electrónico. Escucha en el puerto TCP 110.

Algunos de estos servicios pueden ser altamente personalizados. Por ejemplo, POP3 es un cliente de correo. Los atacantes a menudo sonda de este servicio y, si es vulnerable, el intento de robar cuentas, contraseñas, o incluso el correo electrónico.

Con Specter puede personalizar mensajes de correo electrónico para que los atacantes obtener el servicio POP3 emulado. Con el servidor Web, las organizaciones pueden crear y publicar sus propias páginas Web con su imagen gráfica propia, dando la impresión de que el honeypot es un sistema de producción real. Por ejemplo, reemplazamos la página Web predeterminado para un sistema Solaris con las páginas web de seguimiento de los hackers, el sitio web creado para este libro. Esto le da la flexibilidad para personalizar los servicios emulados, la creación de un honeypot más realista.

3.3.3.4.4. Inteligencia, trampas, los tipos de contraseña, y notificación

Opciones de Inteligencia son una selección de 11 opciones para el honeypot a buscar activamente más información sobre el atacante. Las trampas son similares a los servicios, que son los puertos seleccionados, en la que Specter se escucha. Sin embargo, estos puertos no emular a los servicios sino que se limita registro cualquier conexión. Esto es similar a HBO con la opción falsa Respuestas discapacitados. Usted tendrá que seleccionar los puertos que desea controlar. Specter tiene un puerto opcional séptimo puede configurar para escuchar en cualquier puerto TCP que usted elija. Los seis puertos predefinidos son los siguientes:

- **DNS.** Se utiliza para resolver nombres de dominio o la transferencia de archivos de zona. Escucha en el puerto TCP 53.
- **IMAP4** Mensaje Acceso a Internet de Protocolo. protocolo de texto no cifrado que utilizan los clientes para recuperar el correo electrónico. Escucha en el puerto TCP 143.
- **Portmapper Sun-RPC o Remote Procedure Call**. Escucha en el puerto TCP 111.

- **SSH Secure Shell**. protocolo de cifrado utilizado para la administración remota segura de un sistema o de transferencia de archivos. Escucha en el puerto TCP 22.
- **SUB-7 Windows Troyano**, Escucha en el puerto TCP 27374.
- **BO2K Windows Troya**. Escucha en el puerto TCP 54320.

Escriba la contraseña se utiliza principalmente para engañar a los atacantes. Si el carácter de su equipo trampa se establece en Abrir o extraño, los atacantes potencialmente pueden recuperar un archivo de contraseñas falsas de la trampa. Puede seleccionar el tipo de archivo de contraseñas a los atacantes pueden agarrar cualquier cosa de ser fácil de adivinar las contraseñas en un archivo de contraseña con las contraseñas extremadamente compleja por lo que es mucho más tiempo que consume crack. La intención es que los atacantes para capturar el archivo de contraseñas y perder mucho tiempo de descifrar el contraseñas. Si desea que esta función activada, usted tiene que seleccionar el tipo de contraseña que quieres y permitir que el archivo de contraseñas para ser capturado. Si bien esta característica es entretenido, me siento contraseña captura tiene un valor limitado. La mayoría de los ataques automatizados de derivación archivos de sistema de contraseñas, más fácil la búsqueda de métodos de entrada.

La siguiente categoría es la Notificación-cómo las organizaciones se notifica de un ataque. Siento que esto es una de las secciones más importantes. Honeypots son de poco valor si no puede alertar a la gente apropiada en el momento oportuno. Uno de los rasgos más característicos de Specter son sus amplias opciones de alerta: Viene con cinco opciones, de incidentes de base de datos, correo de alerta, a corto Mail, estado del correo, registro de eventos, y Syslog. Usted puede habilitar como muchas

de estas opciones que desee en cualquier momento. De forma predeterminada, la base de datos de incidentes está habilitada. Esto asegura que toda la actividad detectada es registrada localmente en el equipo trampa y puede ser recuperada más tarde por la característica de Specter LogAnalyzer. Las opciones de notificación a distancia son de Alerta y corto e-mails. Estas opciones proporcionan medios duplicados de recibir las alertas. Condición Jurídica y Social de correo no es un mecanismo de notificación cierto, pero en lugar de estado envía correos electrónicos periódicos a intervalos predeterminados. Para honeypots con poca actividad, estado de estos mensajes de correo electrónico para confirmar que la trampa está aún en funcionamiento.

Dos opciones adicionales de registro son de eventos y Syslog. Los registros de eventos para el sistema operativo de Windows locales donde se puede ver por el visor de sucesos. Syslog registros a un servidor de registro remoto, usando el estándar syslogd (1M) funcionalidad. Si se utiliza Syslog, asegúrese de configurar la prioridad adecuada, instalaciones, y la dirección IP del servidor syslog remoto. Todas estas características son fundamentales para garantizar eficaz y fiable de mecanismos de alerta.

3.3.3.4.5. Opciones adicionales

En el lado derecho de la consola, bajo la ventana de mensajes, son adicionales de configuración y opciones de personalización. La primera opción es para dar al sistema un nombre de host, por lo tanto la personalización de su identidad. A continuación, hay varias opciones para configurar el servidor de correo de direcciones IP y direcciones de correo electrónico para la notificación.

Estas son las críticas a la configuración de la notificación apropiada. Debajo de eso es la opción para la administración remota. Si usted quiere ser capaz de gestionar de forma remota un equipo trampa espectro, debe configurar la dirección IP remota del servidor de administración, determinar qué puerto que desee con la gestión a suceder en adelante, e indicar la contraseña utilizada para la administración remota. Esta funcionalidad es importante para las grandes organizaciones con múltiples honeypots desplegados. Sin embargo, esto no se podrá exigir a las organizaciones que sólo tienen uno o dos implementaciones de Specter. A continuación, puede configurar cualquier IP amigable que puede conectarse a la trampa. Estos son los sistemas de confianza que usted no desea recibir alertas sobre, como su sistema de administración. Esta funcionalidad puede reducir los falsos positivos. Por último, puede configurar el mensaje de advertencia a su ambiente. Si el carácter de su equipo trampa se establece en agresivos, se puede personalizar el mensaje de advertencia que se envía a posibles intrusos.

3.3.3.5. Inicio del Honeypot

Cuando esté listo, inicializar el equipo trampa usando el botón de arranque del motor. Así se inicia la emulación real de honeypot. Una vez que haya configurado el equipo trampa de la manera que desea, puede guardar la configuración en un archivo. De esta manera usted puede configurar varias configuraciones diferentes, salvo que, a continuación, cargar e instalar la configuración de su elección. Specter tiene una variedad de opciones para seleccionar. Son estas opciones que hacen de Specter una solución trampa muy eficaz.

3.3.3.6. Despliegue y mantenimiento de Specter

Specter debe ser instalado manualmente en cualquier sistema que usted quiere ser un honeypot. Esto puede ser un proceso muy intensivo. Sin embargo, Specter tiene una

gran ventaja sobre BOF, ya que pueden ser gestionados de forma remota. Specter viene con una segunda aplicación llamada Specter remoto, que permite a un administrador para gestionar remotamente todos los honeypots Specter.

Para habilitar la administración remota en la trampa a través del menú SpecterControl. Como se señaló anteriormente, es necesario habilitar la opción de gestión remota, configurar el puerto que desea utilizar para la gestión, y le dará la trampa de una contraseña para el acceso remoto. La trampa está listo para la administración remota. Specter tiene una segunda aplicación diseñada específicamente para la administración remota, llamada SpecterRemote. La interfaz gráfica es casi idéntica a SpecterControl, que se utiliza para administrar localmente un sistema. Esto le da la posibilidad de configurar de forma remota y mantener la trampa, como si tuviera acceso local. La única limitación con la administración remota es que no se puede ver de forma remota el honeypot registros almacenados en la base de datos de incidentes, por lo que Log Analyzer no funciona de forma remota.

La capacidad de administrar de forma remota honeypots es crítico para las organizaciones con la intención de desplegar múltiples honeypots. Esto permite a los administradores para colocar los honeypots en una variedad de diferentes áreas de la red, mejorando sus posibilidades de detectar actividad no autorizada.

3.3.3.7. Reunión de información y capacidades de alerta

Hay tres áreas básicas para la detección y recopilación de información con Specter. La primera es de alerta, notificación de una organización cuando el honeypot ha detectado actividad. Specter tiene una funcionalidad de notificación excelente, proporcionando datos eficaz y confiable en tiempo real. El segundo elemento es revisar la información capturada después de ser notificado. Specter admite varios métodos de registro, incluyendo Log Analyzer. Esta es una aplicación independiente que se utiliza para analizar la actividad registra almacenados localmente en el equipo

trampa. El tercer elemento es la recopilación de inteligencia, que es una función única en el honeypot activamente obtener información sobre un atacante.

En el comienzo de este capítulo hemos demostrado cómo Specter puede emular las vulnerabilidades, en este caso un servidor FTP anónimo muestra un atacante FTPing en una trampa que se ha configurado como un sistema abierto, permitiendo al atacante descargar la contraseña del sistema de archivos, en este caso un archivo de contraseñas falsas creadas por Specter. Vamos a examinar este paso de ataque a paso y ver cómo se han detectado y la información registrada para su revisión. Vamos a comenzar con la notificación, cuando se alertó por primera vez al ataque.

Specter admite dos métodos principales de la notificación: a corto Mail y Mail Alert. Vamos a ver cómo nos han alertado a la atacó con cualquiera de esas opciones.

3.3.3.7.1. Breve Correo

Breve Mail es una versión abreviada de alerta de correo. Su finalidad es notificar a las personas a través de buscapersonas o teléfonos celulares, los recursos que se limitan a una pequeña cantidad de caracteres. Su ventaja es que puede ser utilizado para alertar a cualquier persona con acceso a la paginación. Esto significa que su equipo de seguridad realmente puede ir a almorzar y todavía ser notificada. Una desventaja de esto es que la información es limitada: Sólo se informa que el ataque fue detectado. Las organizaciones más probable es que para obtener más información antes de reaccionar ante tal alerta. A continuación vemos la notificación de alerta de correo que habría recibido para el ataque FTP. Tenga en cuenta que no sabemos cuáles son las actividades del atacante son, sólo sabemos que una conexión FTP se hizo.

Date: Sat, 2 Feb 2002 20:56:22 -0600

From: SPECTER on OUTPOST <OUTPOST@honeypot.tracking-hackers.com>

To: lance@spitzner.net

Subject: FTP connection (172.16.1.102) - Attempt 7/16 (FTP/Total)

FTP connection from 172.16.1.102 (FTP attempts: 7, Total attempts: 16)

on Sat Feb 02 20:56:12 2002

3.3.3.7.2. Notificación por correo

Mensajes de alerta son estándar de e-mails que contienen información detallada sobre los ataques. Los administradores son enviados, vía e-mail, información crítica acerca de las sondas de tentativa o compromisos. La ventaja de este mecanismo de alerta es que proporciona una gran cantidad de información sobre el ataque. Las organizaciones pueden responder con rapidez y eficacia, con base en la información de la alerta solo. La desventaja de este mecanismo de alerta es que hay una gran cantidad de información, demasiado para un teléfono celular o buscapersonas. Como tal, sólo puede ser utilizado efectivamente para alertar a un individuo que tiene acceso al correo electrónico. A continuación vemos la notificación de alerta de correo que habría recibido para el ataque FTP. Comparar esta información a la corta de correo que acabamos de revisar. En el corto de correo que ha recibido la información suficiente para determinar que algo estaba pasando, pero no pudo confirmar qué. En el caso de la alerta de correo, puede determinar la intención del intruso, en este caso la recuperación del archivo de contraseñas del sistema. Observe cómo el correo de alerta que nos da el nombre de usuario y la contraseña del atacante. Además, la alerta se explica lo que el atacante está haciendo y cómo está respondiendo Specter.

Date: Sat, 2 Feb 2002 20:56:54 -0600
From: SPECTER on OUTPOST <OUTPOST@honeypot.tracking-hackers.com>
To: lance@spitzner.net
Subject: FTP connection (172.16.1.102) - Attempt 7/16 (FTP/Total)

FTP connection

Host : 172.16.1.102
Login : anonymous
Pass : hax0r
Time : Sat Feb 02 20:56:12 2002

Log:
Client connecting: 172.16.1.102
Client tries anonymous Login
--->331 Guest login ok, send your complete e-mail address as password.
Client sent PASS 'hax0r'
--->230 User anonymous logged in.
Client asks about current directory
--->257 "/" is current directory.
Client set port to 40985, IP to 172.16.1.102
--->200 PORT command successful.
Client asks for directory listing, sending fake listing
--->150 Opening ASCII mode data connection for '/bin/ls'.
Opened data connection to 172.16.1.102 on port 40985, sent directory listing
--->226 Transfer complete.
Client set port to 40986, IP to 172.16.1.102
--->200 PORT command successful.
Client wants to transfer file /etc/passwd
--->150 Opening binary mode data connection for '/etc/passwd'.
Sending passwd file with normal passwords
Transfer of file /etc/passwd to 172.16.1.102 on port 40986 complete.
--->226 Transfer complete.
Client closed connection
--->221 Goodbye.
Closing connection with 172.16.1.102

¿Qué mecanismo de alerta que es mejor para su organización depende de lo que estamos tratando de lograr. Cada uno tiene ventajas y desventajas. Breve Mail es más

accesible, ya que soporta la mayoría de los sistemas de comunicación, incluyendo teléfonos celulares y buscapersonas. Sin embargo, la información es limitada. Con la notificación por correo, que no sólo se notifican a un ataque, pero se le proporciona información detallada sobre la naturaleza del ataque y las actividades del intruso. En algunos casos, es posible que desee utilizar ambos mecanismos de alerta.

Una vez que haya sido notificado del ataque, es posible que desee revisar los registros para obtener más información. Specter es compatible con varios mecanismos de registro, en concreto Log Analyzer, registro de eventos, y syslog.

3.3.3.7.3. Log Analyzer

Specter viene con su propia base de datos integrada para el registro y archivo de las sondas y los ataques. La base de datos se llama la base de datos de incidentes, una de las seis opciones de notificación. Esta base de datos es una colección de archivos de texto, con cada ataque le asigna su propio archivo de texto que registra cada ataque. Log Analyzer es una interfaz gráfica integrada en Specter, que permite consultar y revisar estos archivos de registro. Log Analyzer es lanzado desde la consola principal. Esta utilidad es muy simple, por lo que la consulta de la información y el análisis rápido y fácil. Se empieza por la identificación de la alerta que está interesado y luego haga clic en la entrada de registro respectiva para obtener más información, tales como pulsaciones de teclado del atacante. Log Analyzer proporciona un mecanismo de consulta, lo que le permite consultar y recuperar los ataques basados en el tiempo o su origen. Esto es muy útil para honeypots activos que capturan una gran cantidad de actividad. En la Figura III.13., usando Log Analyzer, que consulta para todos los ataques de FTP. A continuación, identificar el ataque registrado queremos más información acerca de, en este caso la entrada FTP último.

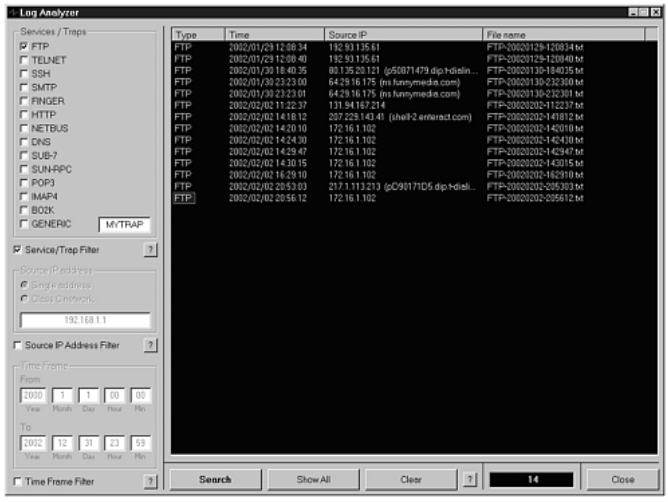

Figura III.19. Análisis de registros

Una vez que haya identificado y seleccionado el incidente sobre el que desea obtener más información, simplemente haga clic en esta entrada. Esto nos lleva a la ventana de información detallada, que se muestra en la Figura III.14. La información en esta ventana es similar a la detallada información en el correo de alerta.

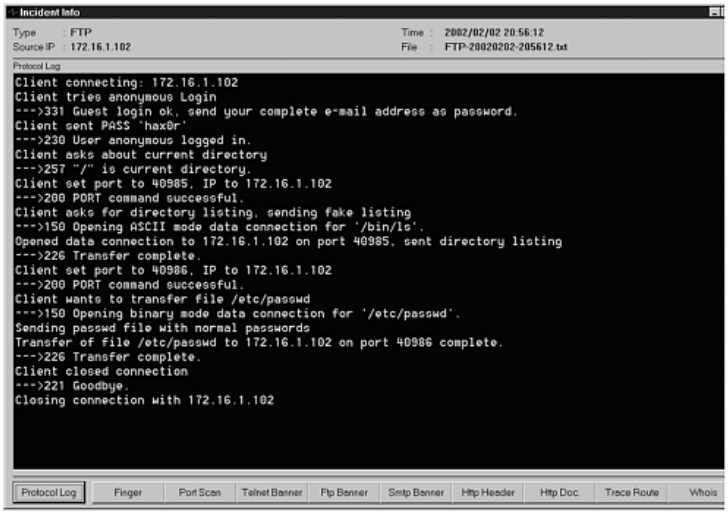

Figura III.20 Detalle del evento seleccionado

La cantidad de información recopilada en cualquier ataque se limita a lo que puede proporcionar servicios emulados, sobre todo las pulsaciones de teclado inicial o de la actividad del atacante cuando relacionada con los servicios emulados. Esta información es crítica para determinar la intención inicial del atacante. Sin embargo, esta información es limitada, ya que no existe un sistema operativo real para el atacante de interactuar con. No aprendemos lo que el atacante tendría que hacer una vez que se tuvo acceso, ni tampoco existe ninguna captura de la actividad de la red. No podemos analizar cualquiera de los rastros del paquete enviado desde o hacia el honeypot. Por último, los servicios emulados están diseñados para capturar e interactuar sólo con ataques conocidos, no está diseñado para capturar la actividad desconocida. Es por eso que considero Specter principalmente un sistema de producción. Sólo se puede reunir una cantidad limitada de información, mientras que un sistema de este tipo pueden obtener niveles muchos mayores de la inteligencia en las acciones del atacante y las intenciones.

3.3.3.7.4. Registro de eventos

Specter apoya otro mecanismo de registro: Registro de sucesos. Este es el nativo para la mayoría de los sistemas Windows, y la actividad de Specter se pueden registrar allí. Desafortunadamente, estos registros tienen poca información, similar a la de correo. No es suficiente para indicar que algo está pasando, pero no mucho más. Esta información se registra específicamente con registros de aplicación. La ventaja de este método es que si usted tiene aplicaciones de tercer seguimiento de estos archivos de registro, estas aplicaciones también se pueden controlar y reaccionar a la actividad Specter.

3.3.3.7.5. Syslog

Syslog es otro método de registro de incidentes capturado por Specter. Esta es una norma de utilidad Unix utilizado para registrar información de un sistema a otro a través de la red. Las ventajas aquí es que se registran ataques que pueden ser recogidos de múltiples honeypots y almacenados de forma centralizada en un servidor de registro remoto. Procesos o aplicaciones en el servidor de registro puede controlar la actividad registra y envía alertas basadas en firmas o actividad específica predeterminada. La desventaja es que las organizaciones tienen que invertir en una arquitectura de servidor syslog para utilizar esta función. En la figura se ve la entrada de syslog que habría recibido para el ataque FTP. La información es similar a la de correo. Con base en esta entrada de registro, tendría suficiente información para cavar un poco más, pero probablemente no lo suficiente para la reacción directa contra el atacante. La ventaja de este método es que si tiene aplicaciones de terceros seguimiento de estos archivos de registro, estas aplicaciones también se pueden controlar y reaccionar a la actividad Specter.

3.3.3.7.6. La Compilación De Datos

No sólo Specter tiene la capacidad de detectar y alertar pasivamente a los ataques, pero también puede obtener información sobre el atacante y el sistema de lanzamiento de los ataques. Specter llama a esta capacidad de inteligencia. Es compatible con hasta 11 opciones diferentes para obtener información de forma activa en cualquier sistema que se conecta a él. El objetivo es obtener conocimiento en tiempo real sobre quién está atacando el honeypot. A menudo, ciertos tipos de información sólo puede obtenerse cuando el ataque está ocurriendo. Estas opciones incluyen el escaneo de puertos que el atacante, tratando de agarrar una bandera de Telnet, o los finger del sistema contrario. Parte de esta información, tales como los dedos, no puede ser capturado después de que el ataque se ha producido, pero sólo mientras que el

atacante está investigando activamente el honeypot. Con esta capacidad de inteligencia, la ubicación o la identidad del atacante puede ser determinado. Una vez capturada, esta información se recupera con el registro de interfaz Analyzer. Estas son las 11 opciones son la recopilación de inteligencia.

- **Finger** sistema remoto de información del usuario.
- **Tracer Finger** de sistemas remotamente conectados al sistema de ataque del honeypot.
- **Portscan** Escaneo remoto del sistema de puertos abiertos. Esta opción lo más probable es que tiene el mayor riesgo de las 11 opciones.
- **Whois** búsqueda en el sistema remoto utilizando ARIN RIPE o bases de datos, acceso a Internet es necesario para esta opción.
- **DNS** resolver el nombre del atacante la dirección IP.
- **Telnet Banner** se conecte al puerto remoto de Telnet en el sistema y obtiene la bandera de inicio de sesión de Telnet.
- **FTP Banner** Conecta al puerto de FTP en el sistema remoto y obtiene la bandera de inicio de sesión FTP.
- **Banner SMTP** se conecta al puerto SMTP en el sistema remoto y obtiene el banner de sendmail.
- **Servidor HTTP** de cabecera Conecta al puerto HTTP en el host remoto y ejecuta el comando HEAD.
- **Documento HTTP** Conecta con el puerto HTTP en el host remoto y las cuestiones del comando GET.
- **Traceroute** Trazado con un host remoto usando ICMP

Sin embargo, existen varios peligros cuando se trata de la recopilación de inteligencia activa. En primer lugar, el honeypot puede alertar al atacante por la consulta activa de la máquina del atacante.

No toda la funcionalidad de inteligencia es tan agresiva como la exploración, pero hay cuestiones que deben considerarse. Depende de la empresa u organización para equilibrar el valor de las medidas de inteligencia activa y el riesgo involucrado.

3.3.3.8. Riesgos asociados con Specter

Como un honeypot de baja interacción, Specter no ofrece ningún sistema operativo real para el atacante para controlar e interactuar. Es extremadamente difícil para el atacante para explotar servicios emulados la trampa y el uso de la trampa de atacar, dañar, o infiltrarse en los sistemas u organizaciones. El mayor riesgo que presenta Specter es el sistema operativo subyacente, ya que debe asegurarse de que las mejores prácticas se siguen para asegurar el sistema operativo en el que será instalado el honeypot. Como tal, lo más probable es que se instale la trampa en un sistema operativo seguro de Windows.

Otro factor de riesgo con Specter se encuentra en las opciones de recogida de información. Como se mencionó anteriormente, las medidas activas de inteligencia puede tener un gran valor, ya que obtener información en tiempo real que puede no estar disponible después del ataque. Sin embargo, estas respuestas automáticas potencialmente puede causar más daño que bien. Existe la posibilidad de un sistema automatizado de análisis para dañar un sistema remoto o una respuesta finger que puede identificar la trampa con una firma de respuesta activa. No hay bien o mal en el uso de materias activas de inteligencia, sino que todo depende de lo que quiere lograr y cuánto riesgo está dispuesto a tomar. Hemos de tener en cuenta que las respuestas automáticas de activos puede tener resultados que no pueden anticipar.

Por último, como hemos mencionado anteriormente, Specter emula los sistemas operativos sólo en el nivel de aplicación, no hay emulación con el subyacente IP. El problema aquí es que el sistema operativo emulado no coincida con la IP. Esta discrepancia potencialmente puede identificar el verdadero propósito de la trampa. Esto no debería ser un problema para la emulación basada en Windows. Desde Specter utiliza la plataforma Windows, Windows emulado honeypots debe tener el buen juego IP. Para ayudar a asegurar que este correcta adecuación, utiliza el exacto mismo sistema operativo subyacente como la trampa de Windows emulado. Si quieres que tu honeypot para parecerse a un sistema Windows XP, utilice una plataforma de Windows XP para su equipo trampa en lugar de Windows NT. Para los sistemas que no sean Windows, esta opción no es posible Como tal, cuando no emular sistemas operativos de Windows, puede ser posible identificar de forma remota las discrepancias entre las aplicaciones de emulación y la base IP.

3.4. Estudio Comparativo

3.4.1. Parámetros de Análisis para el Estudio Comparativo

Parámetro 1: Instalación

Parámetro 2: Seguridad

Parámetro 3: Funcionalidad

Parámetro 4: Portabilidad

Parámetro 5: Soporte Técnico y Situación Legal

3.4.2. Descripción de los Parámetros del Estudio Comparativo

3.4.2.1. Parámetro1: Instalación

En el presente parámetro se llevará a efecto el análisis comparativo de la instalación de cada una de las herramientas de detección de intrusiones no autorizadas en la red Honeyd, BOF, Specter, se comparará los tiempos de ejecución en cada uno de los

pasos de la instalación. Para llevar a efecto la instalación se hará uso del código fuente de la herramienta Honeyd y BOF mediante las herramientas que facilita el sistema operativo Ubuntu con comandos como: sudo apt-get install; y Specter con interfaz gráfica

3.4.2.2. Parámetro 2: Seguridad

En este parámetro se analizará y comparará la seguridad que provee las herramientas de administración de detección de intrusiones en la red Honeyd, BOF, Specter, enfocándose a la prevención de ataques reales a la red por parte del intruso.

3.4.2.3. Parámetro 3: Funcionalidad

En el parámetro funcionalidad se realizará el análisis, y comparación de la generación de los reportes generados por cada una las herramientas de administración de detección de intrusiones en la red Honeyd, BOF, Specter, para la simulación de los sistemas operativos virtuales.

3.4.2.4. Parámetro 4: Portabilidad

La portabilidad se centra especialmente en realizar un análisis comparativo acerca de las herramientas de administración de detección de intrusiones en la red Honeyd, BOF, Specter desde el punto de vista de la facilidad de implantar en las diferentes plataformas o sistemas operativos. Además las aplicaciones extendidas que utilizan el conjunto de funciones que proveen las posibles vulnerabilidades de los sistemas operativos virtuales a los que los intrusos pretenden atacar.

3.4.2.5. Parámetro 5: Soporte Técnico y Situación Legal

Con este parámetro se analizará y comparará la documentación y las condiciones de uso de las herramientas de administración de detección de intrusiones en la red

Honeyd, BOF, Specter. En relación a documentación se tomará en cuenta la información publicada en los sitios oficiales de los respectivos proyectos, la ayuda incorporada a cada herramienta mediante la utilidad MAN. Las condiciones de uso serán analizadas desde el punto de vista de las licencias de distribución y sus restricciones.

3.4.3. Determinación de los indicadores de los parámetros del Estudio Comparativo

Parámetro 1: Instalación

- Personalización
- Información sobre instalación
- Tiempo de descompresión
- Tiempo de compilación
- Tiempo de instalación

Parámetro 2: Seguridad

- Protocolos
- Rastreo de Actividad.
- Vulnerabilidades.

Parámetro 3: Funcionalidad

- Generación de archivos de configuración.
- Generación y análisis de logs.
- Número de conexiones.
- Simulación de Sistemas Operativos.

Parámetro 4: Portabilidad

- Plataformas
- Aplicaciones extendidas

Parámetro 5: Soporte Técnico y Situación Legal

- Ayuda en línea del sitio oficial
- Páginas de ayuda MAN
- Licencias

3.4.4. Descripción de los indicadores de los parámetros del Estudio Comparativo

3.4.4.1. Parámetro 1: Instalación

Personalización

La personalización es un indicador que evaluará el grado de configurabilidad al momento de instalar cada herramienta de administración de detección de intrusiones en la red Honeyd, HBO, Specter. Se evaluará las opciones y argumentos del script config, al momento de realizar la compilación del software.

Información sobre la instalación

Este indicador evaluará la disponibilidad de información adjunta en las distribuciones de cada una de las herramientas de administración de detección de intrusiones en la red Honeyd, HBO, Specter. Específicamente se evaluará la existencia y la estructura de los archivos README e INSTALL, los cuales detallan los pasos para ejecutar una instalación.

Tiempo de descompresión

El tiempo de descompresión se refiere al tiempo que tarda en descomprimirse el código fuente de las herramientas, que por lo general está disponible en formato bz2, gz, tar.gz, .exe, entre otros.

Tiempo de compilación

El tiempo de compilación es el tiempo que toma al script config en compilar el código fuente según las especificaciones y opciones dadas al momento de ejecutar el script en cada herramienta.

Tiempo de instalación

El tiempo de instalación es el tiempo que tarda el comando sudo apt-get install en ubicar los diferentes archivos como pueden ser librerías, cabeceras y ejecutables.

3.4.4.2. Parámetro 2: Seguridad

Protocolos

Este indicador nos permitirá evaluar los protocolos implementados en cada herramienta de administración de detección de intrusiones en la red Honeyd, HBO, Specter, en la transmisión de la información.

Rastreo de Actividad

En el rastreo de actividad, se evaluará la seguridad de los principales logs implementados en cada una de las herramientas de administración de detección de intrusiones en la red Honeyd, HBO, Specter. Para evaluar la seguridad de cada uno de los logs se tomará en cuenta la información de las claves de los principales archivos de configuración implementados.

Vulnerabilidad

Los archivos de configuración implementados en cada una de las herramientas implementadas en cada una de las herramientas de

administración de detección de intrusiones en la red Honeyd, HBO, Specter evaluarán la seguridad en base a los puertos que se encuentren abiertos.

3.4.4.3. Parámetro 3: Funcionalidad

Generación de archivos de configuración

La generación de archivos de configuración desde el punto de vista de la funcionalidad evalúa la calidad de funciones implementadas para cumplir con su propósito en cada herramienta de administración de detección de intrusiones en la red Honeyd, HBO, Specter.

Generación y análisis de logs

Este indicador evaluará las funciones implementadas por cada herramienta para la generación y análisis de los logs basándose en la calidad.

Número de Conexiones

Este indicador evaluará el número de conexiones generadas por cada una de las herramientas de administración de detección de intrusiones en la red Honeyd, HBO, Specter.

Simulación de Sistemas Operativos

Este indicador evaluará el número de sistemas operativos que son capaces de simular los honeypot Honeyd, HBO y Specter.

3.4.4.4. Parámetro 4: Portabilidad

Plataformas

Este indicador evaluará que plataformas son las que soportan las herramientas de administración de detección de intrusiones en la red

Honeyd, HBO, Specter, además se analizará según la información publicada en sus respectivos sitios web oficiales.

Aplicaciones extendidas

El indicador aplicaciones extendidas se refiere a todas las aplicaciones que no pertenecen a cada uno de los proyectos de las herramientas de administración de detección de intrusiones en la red Honeyd, HBO, Specter, aquí se evaluará la cantidad de las aplicaciones externas que las utilizan.

3.4.4.5. Parámetro 5: Soporte técnico y Situación Legal

Ayuda en línea del sitio oficial

Este indicador se basa en la calidad de la información publicada en sitios web por cada herramienta de administración de detección de intrusiones en la red Honeyd, HBO, Specter. Se evaluará dicha información según la estructura que estas presentan.

Páginas MAN

La mayoría de herramientas desarrolladas para las diferentes distribuciones del sistema operativo Linux presentan ayuda mediante la utilidad MAN, por esta razón se evaluará la existencia de esta utilidad en las herramientas de administración de detección de intrusiones en la red Honeyd, HBO, Specter.

Licencias

Este indicador evaluará las libertades de las que gozan cada una de las herramientas de administración de detección de intrusiones en la red

Honeyd, HBO, Specter, se tomará en cuenta los aspectos relacionados con el desarrollo del presente proyecto.

3.4.5. Valorización

Para evaluar los indicadores antes definidos en los módulos correspondientes se empleará la siguiente matriz de valorización con los valores cuantitativos y cualitativos.

Tabla III.VI. Tabla de los valores cualitativos y cuantitativos

Valor cualitativo	Valor cuantitativo
Insuficiente	1
Regular	2
Bueno	3
Muy bueno	4
Excelente	5
NA	Sin valor cuantitativo

Insuficiente

Esta calificación se asignará cuando la herramienta no cumpla con el objetivo del indicador. Dicho de otra manera cuando la herramienta no contenga la característica del indicador. El equivalente en valor cuantitativo será igual a 1.

Regular

Este valor cualitativo se asignará a las herramientas que cumplan de forma deficiente con el objetivo del indicador correspondiente. Su valor cuantitativo será igual a 2.

Bueno

La presente calificación se le asignará a las herramientas que cumplan parcialmente con el objetivo del indicador. El equivalente cuantitativo será igual a 3.

Muy Bueno

El valor cualitativo Muy bueno se asignará a las herramientas que cumpla con casi todos los requerimientos del indicador. El valor cuantitativo será igual a 4.

Excelente

Esta calificación se asignará a las herramientas que cumplan a cabalidad con el objetivo del indicador. Su valor cuantitativo será igual a 5.

NA

Se determina NA cuando el indicador no es aplicable asignar una calificación.

Evaluación de indicadores de los Parámetros del Análisis Comparativo de las Herramientas de administración de detección de intrusiones en la red Honeyd, HBO, Specter

Evaluación de los Indicadores del Parámetro 1: Instalación de las herramientas de administración de detección de intrusiones en la red Honeyd, HBO, Specter

En la tabla III.VII se muestra la calificación que se asignó a los indicadores del Parámetro 1 de las Hherramientas de administración de detección de intrusiones en la red Honeyd, HBO, Specter:

Tabla III.VII. Análisis Comparativo Parámetro 1

Herramientas Indicadores	Honeyd	BOF	Specter
Personalización	Excelente	Regular	Bueno
Información sobre instalación	Muy bueno	Bueno	Regular
Tiempo de descompresión	Muy bueno	Bueno	Bueno
Tiempo de compilación	Excelente	Muy bueno	NA
Tiempo de instalación	Muy Bueno	NA	Muy bueno

Podemos observar en lo referente al indicador Dependencias que las 3 herramientas de administración de detección de intrusiones en la red Honeyd, HBO, Specter son equivalentes debido a que cada herramienta tiene sus propias dependencias como requisito para ser instaladas. El indicador Personalización nos da una idea de flexibilidad de las herramientas, en donde la que se encuentra en bajo nivel es la

herramienta HBO, al igual que el indicador de información sobre la instalación que viene en los archivos README e INSTALL del código fuente de las herramientas. En lo referente a los tiempos observamos que la herramienta más óptima en su instalación es Honeyd seguido de Specter, aunque en la herramienta HBO no se puede aplicar para el tiempo de compilación y el tiempo de instalación.

En la tabla III.VIII. se asigna los valores cuantitativos de acuerdo a la calificación obtenida en los indicadores de cada una de las herramientas de administración de detección de intrusiones en la red:

Tabla III.VIII. Valores Cuantitativos Análisis Comparativo Parámetro 1

	Honeyd	BOF	Specter
Personalización	5	2	3
Información sobre instalación	4	3	2
Tiempo de descompresión	4	3	3
Tiempo de compilación	5	4	0
Tiempo de instalación	4	0	4
Total	26	12	12

Análisis Comparativo del Parámetro 1: Instalación de las las herramientas de administración de detección de intrusiones en la red Honeyd, HBO, Specter, se observa claramente el mejor performance de la herramienta Honeyd, seguido de la herramienta HBO y por último HBO y Specter toman valores iguales para el mencionado parámetro.

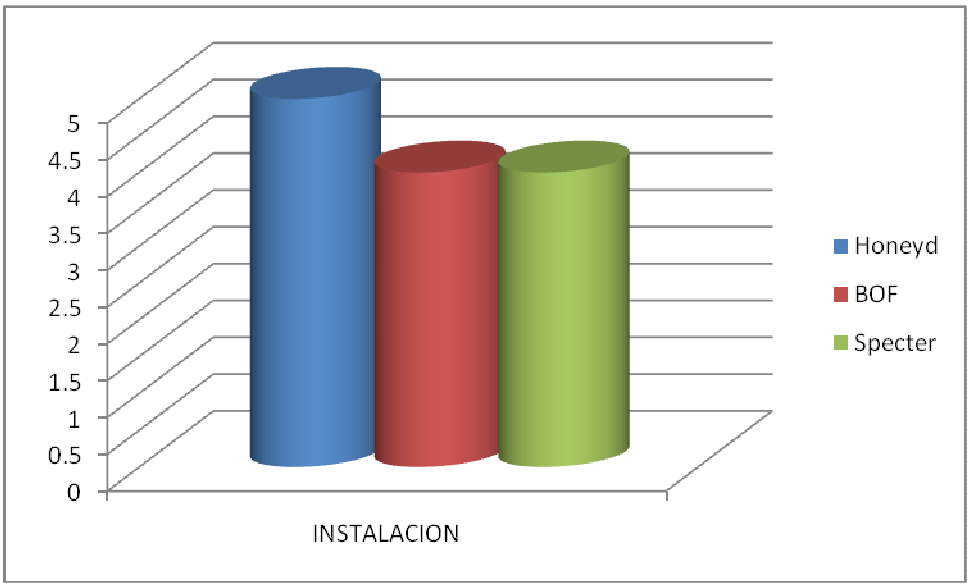

Figura III.21. Gráfico Estadístico Análisis Comparativo Parámetro 1

Evaluación de los Indicadores del Parámetro 2: Seguridad de las Herramientas de administración de detección de intrusiones en la red Honeyd, HBO, Specter

El análisis comparativo del Parámetro 2 lo resumimos en la siguiente tabla:

Tabla III.IX. Análisis Comparativo Parámetro 2

Herramientas / Indicadores	Honeyd	BOF	Specter
Protocolos	Excelente	Muy Bueno	Muy Bueno
Rastreo de Actividad	Excelente	Bueno	Muy Bueno
Vulnerabilidad	Muy Bueno	Bueno	Muy Bueno

En este parámetro existe casi una igualdad en la evaluación de los indicadores, ya que las dos herramientas Honeyd y Specter utilizan varios puertos para que el intruso pueda realizar los ataques.

En la siguiente tabla se asigna la equivalencia cuantitativa obtenida del Análisis Comparativo del Parámetro 2:

Tabla III.X. Valores Cuantitativos Análisis Comparativo Parámetro 2

Herramientas / Indicadores	Honeyd	BOF	Specter
Protocolos	5	4	4
Rastreo de Actividad	5	3	4
Vulnerabilidad	4	4	4
Total	14	11	12

A continuación resumiremos el análisis comparativo del Parámetro 2 Funcionalidad de las Herramientas de administración de detección de intrusiones en la red Honeyd, HBO, Specter

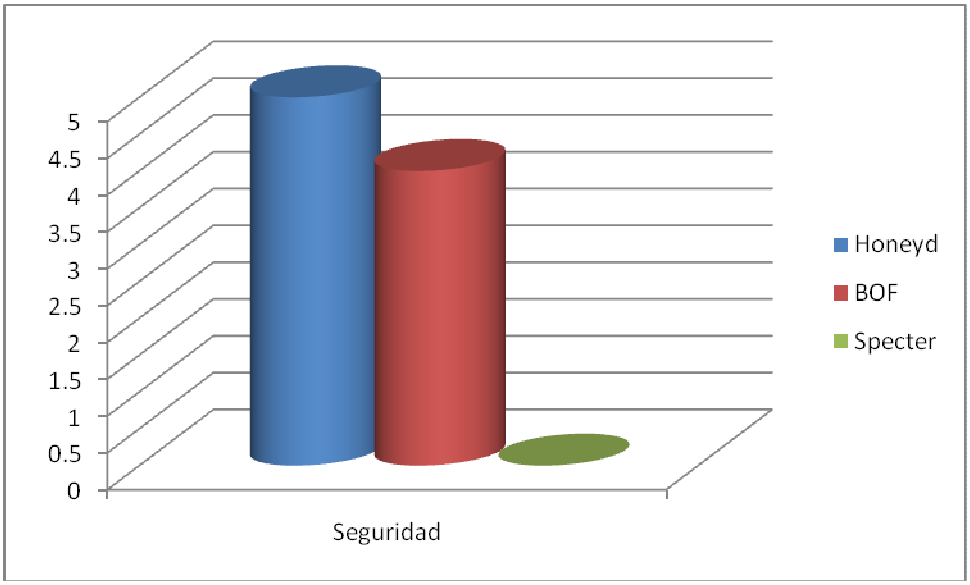

Figura III.22. Gráfico Estadístico Análisis Comparativo Parámetro 2

Evaluación de los Indicadores del Parámetro 3: Funcionalidad de las Herramientas de administración de detección de intrusiones en la red Honeyd, HBO, Specter.

El análisis comparativo del Parámetro 3 lo resumimos en la siguiente tabla:

Tabla III.XI. Análisis Comparativo Parámetro 3

Herramientas / Indicadores	Honeyd	BOF	Specter
Generación de archivos de configuración	Excelente	Muy Bueno	Bueno
Generación y análisis de logs	Excelente	Muy Bueno	Bueno
Número de conexiones	Excelente	Bueno	Muy Bueno
Simulación de S.O	Excelente	Bueno	Muy Bueno

La funcionalidad en la generación de archivos de configuración es mejor en la herramienta Honeyd ya presenta muchos formas para la generación de sistemas operativos virtuales personalizados, presenta mayor documentación y ayuda que las demás.

La generación y análisis de logs de igual forma Honeyd posee mayor cantidad de detecciones y ayuda, además las opciones de configuración en la generación es mayor.

La cantidad de conexiones en la herramienta Honeyd es mucho mayor que las generadas por HBO y Specter ya que manejan menos número de conexiones en tiempo real. Así mismo Honeyd emite muchas más simulaciones de sistemas operativos virtuales.

A continuación se muestra la equivalencia cuantitativa resultado del Análisis Comparativo del Parámetro 3:

Tabla III.XII. Valores Cuantitativos Análisis Comparativo Parámetro 3

Herramientas / Indicadores	Honeyd	BOF	Specter
Generación de archivos de configuración	5	4	3
Generación y análisis de logs	5	4	3
Número de conexiones	5	3	4
Simulación de S.O	5	3	4
Total	20	14	14

Aquí se representa gráficamente el análisis comparativo del parámetro 3: Funcionalidades las Herramientas de administración de detección de intrusiones en la red Honeyd, HBO, Specter.

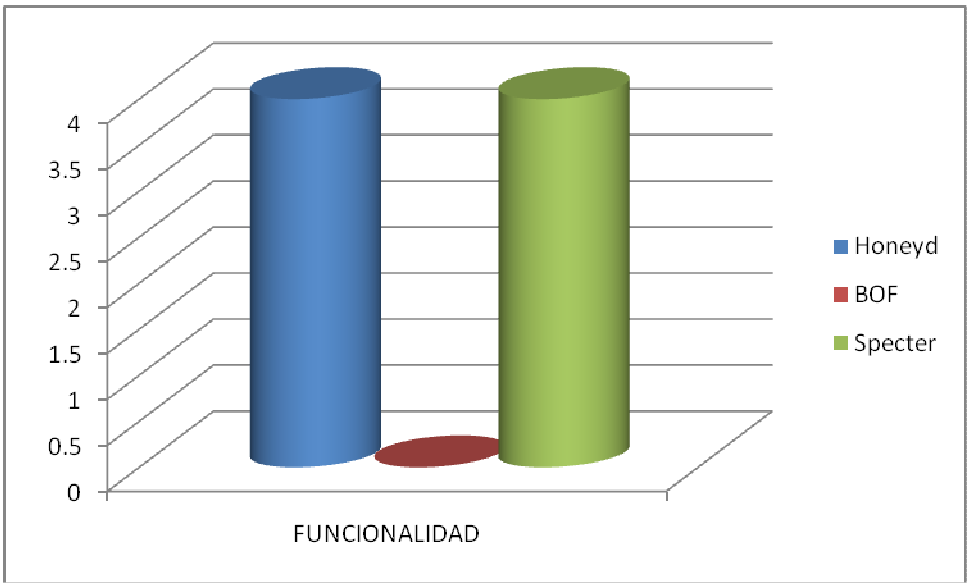

Figura III.23. Gráfico Estadístico Análisis Comparativo Parámetro 3

Evaluación de los Indicadores del Parámetro 4: Portabilidad de las Herramientas de administración de detección de intrusiones en la red Honeyd, HBO, Specter

El análisis comparativo del Parámetro 4 lo resumimos en la siguiente tabla:

Tabla III.XIII. Análisis Comparativo Parámetro 4

Herramientas / Indicadores	Honeyd	BOF	Specter
Plataformas	Excelente	Bueno	Bueno
Aplicaciones extendidas	Excelente	Muy Bueno	Bueno

Honeyd está diseñado para ser implantado en mayor número de plataformas y aunque las otras herramientas también son multiplataforma Honeyd tiene una gran ventaja.

Está muy claro que la herramienta Honeyd por mayor tiempo en funcionamiento es la que mayor información tiene disponible y por la misma razón es la que hasta la actualidad se la ha mejorado en el desarrollo de aplicaciones seguras.

En la siguiente tabla se asigna los valores cuantitativos de acuerdo a la calificación obtenida en el análisis comparativo del Parámetro 4:

Tabla III.XIV. Valores Cuantitativos Análisis Comparativo Parámetro 4

Herramientas / Indicadores	Honeyd	BOF	Specter
Plataformas	5	3	3
Aplicaciones extendidas	5	4	3
Total	10	7	6

A continuación se muestra la representación gráfica del Parámetro 4: Portabilidad de las Herramientas de administración de detección de intrusiones en la red Honeyd, HBO, Specter

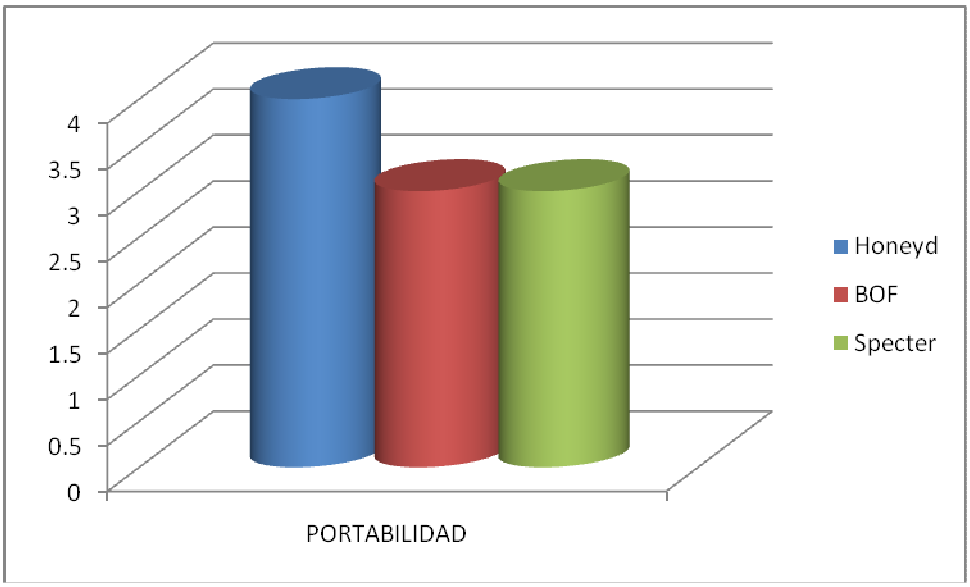

Figura III.24. Gráfico Estadístico Análisis Comparativo Parámetro 4

Evaluación de los Indicadores del Parámetro 5: Soporte Técnico y Situación Legal de las Herramientas de administración de detección de intrusiones en la red Honeyd, HBO, Specter

El análisis comparativo del Parámetro 5 lo resumimos en la siguiente tabla:

Tabla III.XV. Análisis Comparativo Parámetro 5

Herramientas / Indicadores	Honeyd	BOF	Specter
Ayuda en línea del Sitio Oficial	Excelente	Bueno	Muy bueno
Páginas de ayuda MAN	Excelente	Bueno	Muy Bueno
Licencias	Excelente	Muy Bueno	Bueno

Podemos observar que la herramienta que contiene una mejor estructura de ayuda en línea de su sitio web oficial es la herramienta Honeyd, debido a que en ella no solo contiene documentación de información de la herramienta como tal sino también información de las librerías principales que utiliza la herramienta Honeyd y documentación de los conceptos teóricos que se necesita conocer acerca de dicha herramienta. En relación a la utilidad MAN se puede observar que el único caso especial es en la herramienta HBO debido a que no existen muchas páginas para realizar el análisis comparativo. La única herramienta que contiene restricciones explícitas acerca de su código fuente es la herramienta Specter ya que para poder implementar esta herramienta se tiene que adquirir las respectivas licencias. En términos generales en lo referente al indicador Licencias las herramientas Honeyd y HBO se encuentran bajo código libre, debido a que ninguna de ellas restringe la utilización de sus respectivas herramientas.

A continuación se puede apreciar su equivalencia cuantitativa del Análisis comparativo del Parámetro 5:

Tabla III.XVI. Valores Cuantitativos Análisis Comparativo Parámetro 5

Herramientas / Indicadores	Honeyd	BOF	Specter
Ayuda en línea del Sitio Oficial	5	3	4
Páginas de ayuda MAN	5	3	4
Licencias	5	4	3
Total	15	10	11

Aquí se representa gráficamente el análisis comparativo del Parámetro 5: Soporte Técnico y Situación Legal de las Herramientas de administración de detección de intrusiones en la red Honeyd, HBO, Specter.

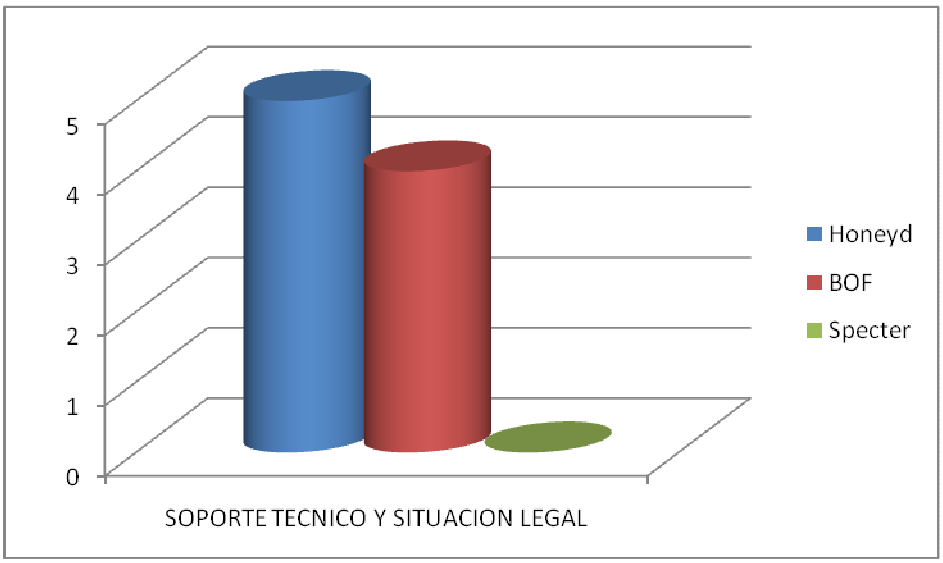

Figura III.25. Gráfico Estadístico Análisis Comparativo Parámetro 5

Matriz de Valorización: Análisis Comparativo de los Indicadores de los Parámetros de las Herramientas de administración de detección de intrusiones en la red Honeyd, HBO, Specter

Luego de experimentar el comportamiento de cada una de las Herramientas de administración de detección de intrusiones en la red Honeyd, HBO, Specter, podemos cuantificar la calificación de los indicadores de los 5 parámetros que conforman el análisis comparativo, a continuación se presenta la matriz de valorización:

Tabla III.XVII. Matriz de Valorización Análisis comparativo de las herramientas OpenSSL, GnuTLS y NSS

Herramientas Indicadores	Honeyd	BOF	Specter
Personalización	5	2	3
Información sobre instalación	4	3	2
Tiempo de descompresión	4	3	3
Tiempo de compilación	5	4	0
Tiempo de instalación	4	0	4
Protocolos	5	4	4
Rastreo de Actividad	5	3	4
Vulnerabilidad	4	4	4
Generación de archivos de configuración	5	4	3
Generación y análisis de logs	5	4	3
Número de conexiones	5	3	4
Simulación de S.O	5	3	4
Plataformas	5	3	3
Aplicaciones extendidas	5	4	3
Ayuda en línea del Sitio Oficial	5	3	4
Páginas de ayuda MAN	5	3	4
Licencias	5	4	3
Total	81	55	56

Haciendo uso de la estadística analítica podemos representar gráficamente el total de los valores cuantitativos de los parámetros del análisis comparativo de las Herramientas de administración de detección de intrusiones en la red Honeyd, HBO, Specter

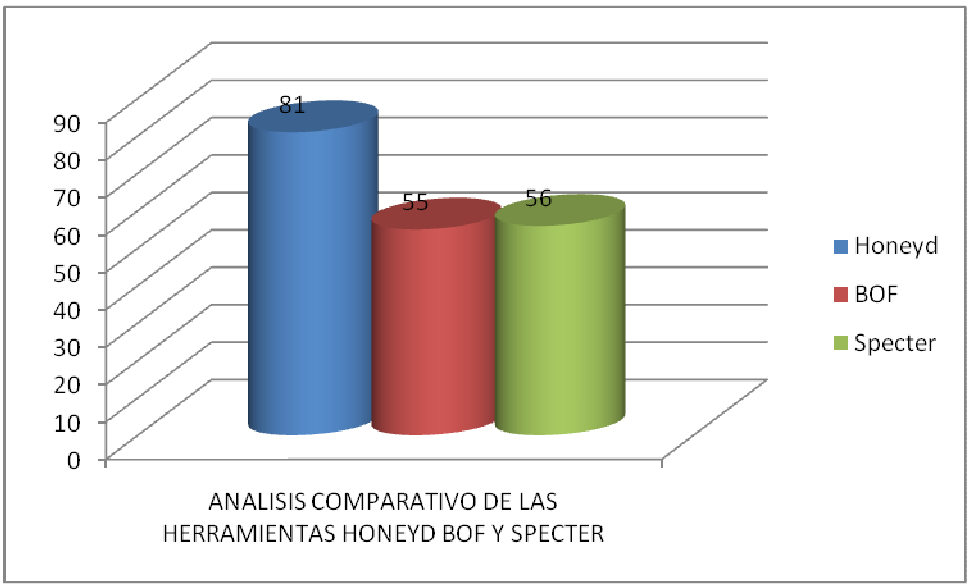

Figura III.26. Gráfico Estadístico Análisis Comparativo de las Herramientas Honeyd, BOF y Specter

Mediante la figura III.26 muestra mediante el diagrama de barras simple la sumatoria obtenida por la tabulacón de todos los indicadores de los parámetros, determinándose como herramienta más funcional y que mejora la seguridad para la detección de intrusiones en la red es Honeyd que alcanzo un total de 81 puntos a diferencia de BOF y Specter que obtuvieron 55 y 56 respectivamente. Lo que quiere decir que Honeyd es la herramienta más operativa.

3.5. Comprobación de la hipótesis

La hipótesis del presente estudio planteo que:

La implementación de un sistema de detección y análisis de intrusiones no autorizadas mediante el uso de Honeypots, permitirá conocer de mejor manera el comportamiento de los intrusos y mejorar la seguridad de la red.

Verificación de la Hipótesis

Para verificar si la hipótesis se acepta o se niega, se debe separar en 2 variables, dependiente e independiente, como se indica a continuación:

Variable Independiente: La implementación de un sistema de detección y análisis de intrusiones no autorizadas

Variable Dependiente: Comportamiento de intrusos y mejora de la seguridad en la red.

Indicadores de comprobación

- Vulnerabilidad
- Rastreo de actividad
- Nivel de intrusiones
- Eficiencia de la red
- Generaciones de Logs

Los valores cualitativos que se utilizo para evaluar los indicadores son los siguientes:

Valor Cualitativo	Valor Cuantitativo
Malo	1
Regular	2
Bueno	3
Muy Bueno	4
Excelente	5

Tabla III.XVIII. Tabla de Contingencia

Indicadores	Sin HD Fo	Con HD Fe	(Fo - Fe)^2/Fe
Vulnerabilidad	2	4	1
Rastreo de Actividad	1	5	3.2
Nivel de Instrucciones	1	4	2.25
Eficiencia de la Red	2	4	1
Generaciones de Logs	1	5	3.2

La prueba aplicada para nuestro caso fue la χ^2 de Pearson (pronunciado como "ji-cuadrado" y a veces como "chi-cuadrado) es considerada como una prueba no paramétrica que mide la discrepancia entre una distribución observada y otra teórica (bondad de ajuste), indicando en qué medida las diferencias existentes entre ambas, de haberlas, se deben al azar en el contraste de hipótesis.

La fórmula que da el estadístico es la siguiente:

Valores para calcular x^2

Datos	Valores
Columnas (k)	2
Renglones (r)	5
Grados de libertad (r-1)*(k-1)	4
Alfa	0,05
ji cuadrado	10,65
Valor crítico para F (una cola)	9.49

La tabla muestra los datos estadísticos de nuestra hipótesis. A la vista de este resultado, lo que tenemos que hacer ahora es plantear un contraste de hipótesis.

Planteamiento de Hipótesis para comprobar si existe diferencia significativa entre las Herramientas de administración de detección de intrusiones en la red

H0= La implementación de un sistema de detección y análisis de intrusiones no autorizadas mediante el uso de Honeypots, no permitirá conocer el comportamiento de los intrusos ni mejorará la seguridad de la red.

H1= La implementación de un sistema de detección y análisis de intrusiones no autorizadas mediante el uso de Honeypots, permitirá conocer de mejor manera el comportamiento de los intrusos y mejorar la seguridad de la red.

Bajo la hipótesis nula de independencia, se sabe que los valores del estadístico x^2 se distribuyen según una distribución conocida denominada ji-cuadrado, que depende de un parámetro llamado “grados de libertad” (g.l.). Para el caso de una tabla de contingencia de r filas y k columnas, los g.l. son igual al producto del número de filas menos 1 (r-1) por el número de columnas menos 1 (k-1) (Valores obtenidos de la Tabla de Valoración)

Para nuestro caso el valor del Grado de Libertad es 4

De ser cierta la hipótesis nula, el valor obtenido debería estar dentro del rango de mayor probabilidad según la distribución ji-cuadrado correspondiente. El valor-p que usualmente reportan la mayoría de paquetes estadísticos no es más que la probabilidad de obtener, según esa distribución, un dato más extremo que el que proporciona el test o, equivalentemente, la probabilidad de obtener los datos observados si fuese cierta la hipótesis de independencia. Si el valor-p es muy pequeño (usualmente se considera $p<0.05$) es poco probable que se cumpla la hipótesis nula y se debería de rechazar.

De este modo, si el estadístico calculado del experimento toma un valor de 10.65, y el valor crítico estandarizado de x^2 es 9.49

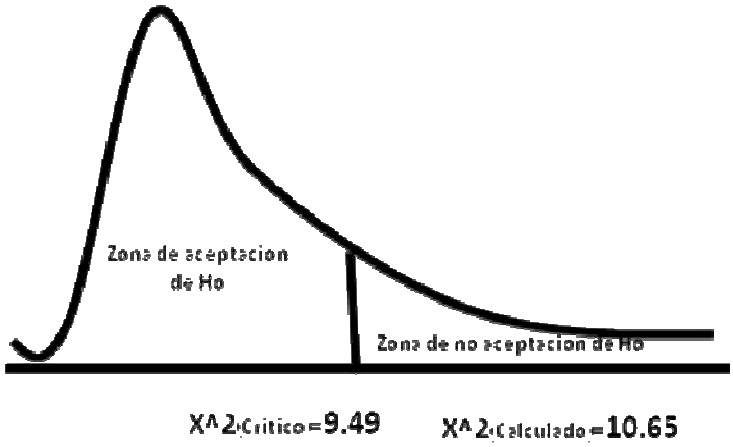

Figura III.27. Grafica de aceptación de la hipótesis

Siendo que el valor Chi cuadrada (c 2) obtenido es mayor que el valor crítico, se concluye que “La implementación de un sistema de detección y análisis de intrusiones no autorizadas mediante el uso de Honeypots, permitirá conocer de mejor manera el comportamiento de los intrusos y mejorará la seguridad de la red.

CAPÍTULO IV

4. IMPLEMENTACIÓN DE LA TECNOLOGÍA DE DETECCIÓN DE INTRUSIONES MEDIANTE HONEYPOTS

4.1. Introducción

El objetivo fundamental de un honeypot es simular frente a los atacantes un sistema virtual que aparentemente para ellos es real, para lograr esto se utilizan servicios también simulados los cuales son muy llamativos para el intruso, estos servicios crean una distracción frente a sistemas reales y hacen pensar al atacante que está cumpliendo con su objetivo. Se pueden simular gracias al Honeyd una gran variedad de sistemas de paga o libres, con una infinidad de servicios, al mismo tiempo en caso de tener sistemas IDS como es el caso del DESITEL puede continuar detectando la actividad del enemigo. El honeypot recopila información en archivos log y txt mientras está siendo atacado, para de esta forma utilizar la información de una manera proactiva en la prevención de intrusiones similares, pueden ser analizadas para conocer la forma y las herramientas que usa un intruso para vulnerar la red de la institución, además de sus debilidades y necesidades en lo relacionado a seguridad. De esa manera los ataques se efectuarán sobre ese sistema sin causar ningún daño al

sistema real incluso se puede lograr configurar otro equipo para que reciba los logs en la red y de esta forma tener segura la información que se recopiló sobre el ataque. El Honeypot no es un sistema de protección de la red específicamente ni un IDS pero es un complemento para la seguridad de una red, es un medio de distracción como su mismo nombre lo indica y es un repositorio de eventos de intrusión dentro de la red real. Es el software y hardware, real y simulado, cuya intención es atraer (como la miel) a los atacantes, simulando ser sistemas débiles o con fallas de seguridad no del todo evidentes, pero si lo suficiente para atraerlos y ser un reto para las habilidades del atacante. Se basa en la idea de "conocer al enemigo" para poder combatirlo.

4.2. Honeyd

Honeyd es un honeypot de baja interacción. Desarrollado por Niels Provos, Honeyd es OpenSource y está diseñado para correr principalmente en sistemas Unix (aunque fue portado a Windows). Honeyd trabaja en el concepto del monitoreo del espacio IP no utilizado. Cualquier instante que observa un intento de conexión a un IP no utilizado, éste intercepta la conexión e interactúa con el atacante, pretendiendo ser la víctima. Por defecto, Honeyd detecta y loguea cualquier conexión a cualquier puerto UDP o TCP. Como si fuera poco, se pueden configurar a los servicios emulados para que monitoreen puertos específicos, como un servidor FTP emulado monitoreando el puerto TCP 21. Cuando un atacante conecta al servicio emulado, el honeypot no sólo detecta y loguea la actividad, sino que captura también toda la actividad del atacante con el servicio emulado. En caso del servidor FTP emulado podemos potencialmente capturar el login y password, los comandos que ingresa y quizás también descubrir lo que está buscando o su identidad. Todo depende del nivel de emulación del honeypot. La mayoría de los servicios emulados trabajan de la misma manera. Ellos esperan un tipo específico de comportamiento, y están programados para reaccionar en una forma predeterminada. Si el ataque A hace esto, entonces reaccionan de este modo. Si el

ataque B hace aquello, entonces responden del otro modo. La limitación está en que si el atacante hace algo que la emulación no tiene previsto, entonces no saben cómo responder. La mayoría de los honeypots de baja interacción, incluyendo Honeyd, simplemente genera un mensaje de error. Podrá ver cuáles son los comandos que soporta el servidor FTP emulado de Honeyd viendo el código fuente.

4.2.1. Características de honeyd

- Honeyd es un honeypot de baja interacción.
- Simula a millares de anfitriones virtuales al mismo tiempo.
- No solo puede simular sistemas Linux o Windows sino también equipos de red, es decir Honeyd puede aparentar ser un router Cisco, un webserver WinXP o un servidor DNS Linux, etc.
- Configuración de servicios arbitrarios vía su simple archivo de configuración
- Uso de templates para emular los OS's.
- Uso de fingerprinting.
- Uso de la base de datos de fingerprints de Nmap.
- Simula sistemas operativos en el nivel de TCP/IP.
- Simulación de las topologías arbitrarias del enrutamiento.
- Virtualización del subsistema.

4.2.2. Requisitos para la instalación de honeyd

Para lograr la instalación de honeyd son necesarias varias librerías las cuales se describen a continuación.

Libdnet

Esta librería que proporciona una interfaz portátil simplificada para varias rutinas de red de bajo nivel, incluyendo ARP del núcleo y la manipulación de la tabla de ruteo, firewalling, configuración de la interfaz, la manipulación de direcciones de red, túneles IP y la transmisión de datagramas IP. Libdnet es licenciado y distribuido bajo los términos de la Licencia BSD.

Libevent

El libevent API proporciona un mecanismo para ejecutar una función de devolución de llamada, cuando ocurre un evento específico en un descriptor de archivo o después de que un tiempo de espera se ha alcanzado. Además, también admiten devoluciones de llamada libevent debido a las señales de los tiempos de espera o regular.

Libevent pretende reemplazar el bucle de eventos que se encuentran en servidores de la red. Una aplicación sólo debe llamar a event_dispatch () y luego agregar o quitar eventos de forma dinámica sin tener que cambiar el bucle de eventos.

Como resultado, libevent permite el desarrollo de aplicaciones portátiles y proporciona el mecanismo de notificación de eventos más escalable disponible en un sistema operativo. Libevent también se puede utilizar para aplicaciones multi-threaded.

Libevent es una biblioteca multiplataforma y debe recopilar en Mac OS X, Linux, BSD, Solaris y Windows.

Libpcap

Llibpcap es una interfaz independiente del sistema para capturar paquetes a nivel de usuario. Llibpcap proporciona un marco portátil para monitoreo de red de bajo nivel. Las aplicaciones incluyen seguimiento de la seguridad, la depuración de la red, red de recogida de estadísticas, etc.

4.2.3. Beneficios de la implementación de honeyd

- **Genera un pequeño volumen de datos:** Honeyd al no ser utilizado como equipo de producción, generan pocos datos pero de altísimo valor, al contrario de un IDS (Sistema de detección de intrusos) mal configurado que generan cientos de megas de información que a veces pueden ser “inútiles”, u otras herramientas que generarían “logs” de sistema con datos innecesarios.

- **Mínimos Recursos Requeridos:** A diferencia de otros sistemas de seguridad, las necesidades de Honeyd son mínimas. No consume ni ancho de banda ni memoria o CPU extra. No necesita complejas arquitecturas o varios ordenadores centralizados, cualquier ordenador conectado a la red puede realizar este trabajo.

- **Inexistencia de Falsas alarmas:** Las características de los sistemas trampa elimina la existencia de actividad normal o de producción en los mismos. Estas herramientas de seguridad deben recibir únicamente actividades sospechosas. Esto reduce significativamente el número de falsos positivos (alarma cuando no existe ataque) y falsos negativos (omisión de alarma cuando hay verdaderamente un ataque).

- **Universalidad:** Este tipo de sistemas sirven tanto para posibles atacantes internos como externos. De esta forma, obviamente, se ha de evitar poner a las máquinas nombres como “honeypot” o “attack-me”. Su objetivo es pasar desapercibidas en una red como una máquina más.

- **Simplicidad:** Uno de los puntos más importantes a favor de los sistemas trampa es su sencillez. No utilizan complicados algoritmos de análisis, ni rebuscados métodos para registrar la actividad de los intrusos. Por el contrario, sólo hay que instalarlos y esperar. Algunos sistemas trampa de desarrollo pueden poseer mayor nivel de complejidad, pero no comparable a otros enfoques.

- **IPv6:** Uno de los problemas que presentan algunas herramientas de seguridad es que no soportan el protocolo IPv6, sucesor del actual IPv4 ampliamente utilizado en Internet. Este protocolo está siendo principalmente utilizado en países asiáticos como Japón. Utilizar IPv6 utilizando túneles sobre IPv4, como hacen algunos atacantes, puede imposibilitar la detección por parte de muchos sistemas de detección. No obstante, los sistemas trampa registran toda la actividad ocurrida, por lo que se pueden identificar este tipo de ataques.

- **Reutilización:** La mayoría de los productos de seguridad necesitan mantener al día sus mecanismos de detección y defensa para mantener su efectividad. Si no se renuevan, dejan de ser útiles. No obstante, los sistemas trampa, debido a su propia naturaleza, siempre serán de ayuda independientemente del tiempo que pase, siempre habrá atacantes dispuestos a comprometer estos sistemas

de una u otra forma, mostrando el nivel de actividad de este sector y los métodos que utilizan.

4.2.4. Desventajas de la implementación de honeyd

- **Equipos pasivos:** Los sistemas trampa carecen de utilidad y valor, si no reciben ataques. Si un atacante detecta uno de estos sistemas lo tornará ineficiente, porque no ejecutará atentados inclusive estando en la misma red de sistemas de producción que si pueden ser objetos de ataques.

- **Fuente potencial de riesgo:** Debido a la atracción de atacantes, se debe tener cuidado en la configuración, y convertirlo en un entorno cerrado y controlado (jailed envinronment), para evitar que se utilice como fuente de ataque a otros sistemas, y al propio.

- **Finger print:** Es la identificación local o remota de un sistema o servicio. Es posible que la deficiente implementación de un sistema trampa lo delate, haciéndolo reconocible ante un intruso, lo que como se dijo lo volverá inútil, o se lo puede utilizar para desviar la atención de la administración de seguridad.

4.3. Establecimiento de políticas para la implementación

Para establecer una correcta configuración del honeypot debemos analizar el diagrama de la red.

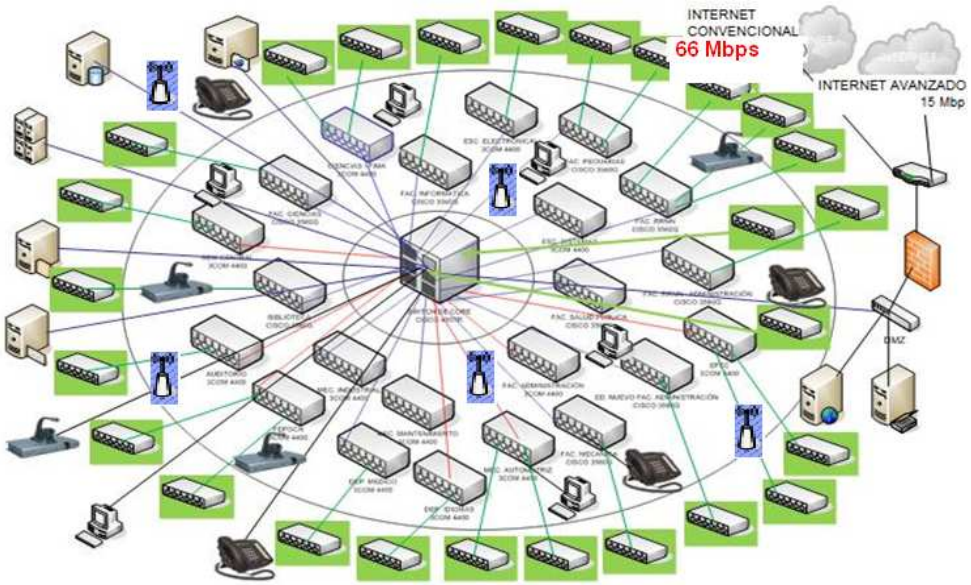

Figura IV.28 Crecimiento tecnológico ESPOCH

De acuerdo al diagrama de la figura IV.28, a los conceptos del proyecto honeypot, y a los criterios tomados para la simulación procedemos con los siguientes pasos previos a la elaboración del script que ejecute las políticas del firewall.

a) Establecer el grupo de clientes llamadas zonas, donde se incluye el propio firewall, y son:

- Internet (usuario externo: cliente o atacante)(INT)
- Zona desmilitarizada (En esta zona se instala el honeypot)(HON)
- Red interna de la ESPOCH(RED)
- Firewall(FW)

El diagrama de las zonas establecidas y su nomenclatura se refieren a la figura IV.28

Lista de servicios que el firewall va a atender:

Tabla IV.IX. Servicios que permitirá el Firewall

Servicio	Puerto
Telnet	23
HTTP	80
SSH	22
Ping	-

Establecer relaciones entre las zonas, con esto se establece si una zona es cliente o servidor de otra, por consecuencia si hay tráfico y en qué sentido:

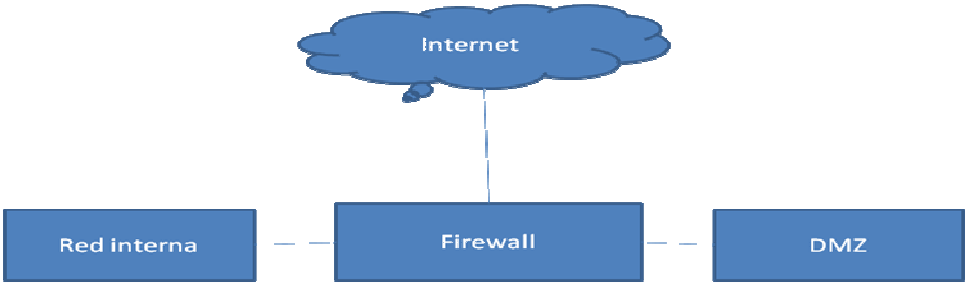

Figura IV.29. Diagrama de zonas para el Firewall

Tabla VI.X. Tráfico entre zonas

Cliente	Servidor	Tráfico
INT	FW	✓
INT	RED	✓
INT	HON	✓
FW	INT	X
FW	RED	✓
FW	HON	✓
SER	FW	✓
SER	INT	✓
SER	HON	x
HON	INT	x
HON	FW	x
HON	RED	x

Según la tabla VI.X. se puede observar el flujo del tráfico que va a existir en la estructura de la red para tener una guía al momento de crear el script de configuración del honeypot, además en la Figura IV.X. se observa con más sencilles el lugar en donde va a estar ubicado el honeypot, lo más recomendable es la DMZ.

Para nuestro ejemplo vamos a emular 3 equipos con los respectivos servicios que ofrecerán al atacante:

- **Computador con Microsoft Windows XP Home Edition**

  Telnet: Puerto # 23

  SSH: Puerto # 22

  FTP: Puerto # 21

  ICMP activado

- **Equipo Open** Suse 8.0.- sistema operativo Linux que va a ser simulado en el honeyd.

  Telnet: Puerto # 23

  SSH: Puerto # 22

  FTP: Puerto # 21

  HTTP: Puerto # 80

  ICMP activado

- **Equipo Microsoft Windows 2000 Server SP3**

  FTP: Puerto # 21

  Telnet: Puerto # 23

  ICMP activado

4.4. Instalación de Honeyd

Para realizar la instalación de honeyd vamos a realizar el sistema operativo Ubuntu 10.10 por ser una versión estable, completa y moderna del sistema Linux, además se ha escogido dicho sistema operativo por la facilidad con la que se puede instalar aplicaciones adicionales al sistema.

El instalador e información sobre honeyd se encuentra en la página oficial del honeypot http://www.honeyd.org.

El primer paso es realizar la instalación de Honeyd para lo cual vamos a utilizar el comando que se detalla a continuación, cabe recalcar que para poder realizar la instalación y la utilización de varios archivos tenemos que ser superusuarios:

Comandos utilizados

usuario@usuario:$ su

contraseña: **********

root@usuario:/home/usuario#

Para instalar honeyd sobre el sistema operativo usamos el siguiente comando, con el cual se descargaran los instaladores y las librerías necesarias para el correcto funcionamiento del honeypot desde los repositorios de Ubuntu:

root@usuario:/home/usuario# sudo apt-get install honeyd

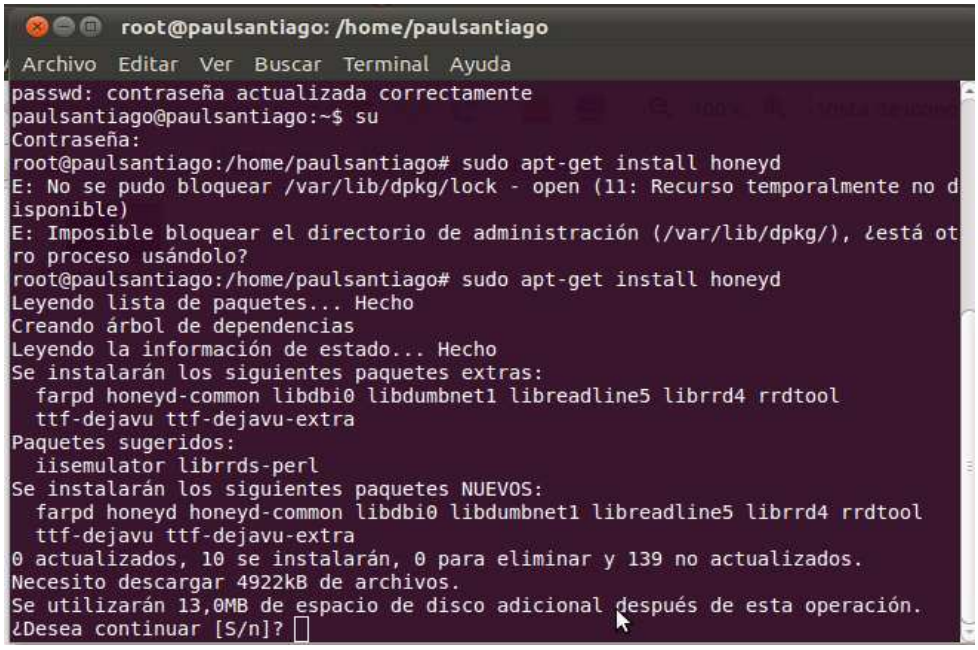

Figura IV.30. Captura de instalación de honeyd

Se puede ver que inmediatamente luego de ejecutar el comando la distribución Ubuntu empieza a descargarse el sistema Honeyd y a instalar varias librerías y dependencias. El honeypot solo estará instalado si al finalizar el porcentaje del proceso nos indica que ha sido instalado con éxito y si existe algún error en el proceso de instalación de igual manera se mostrara un mensaje de instalación fallida.

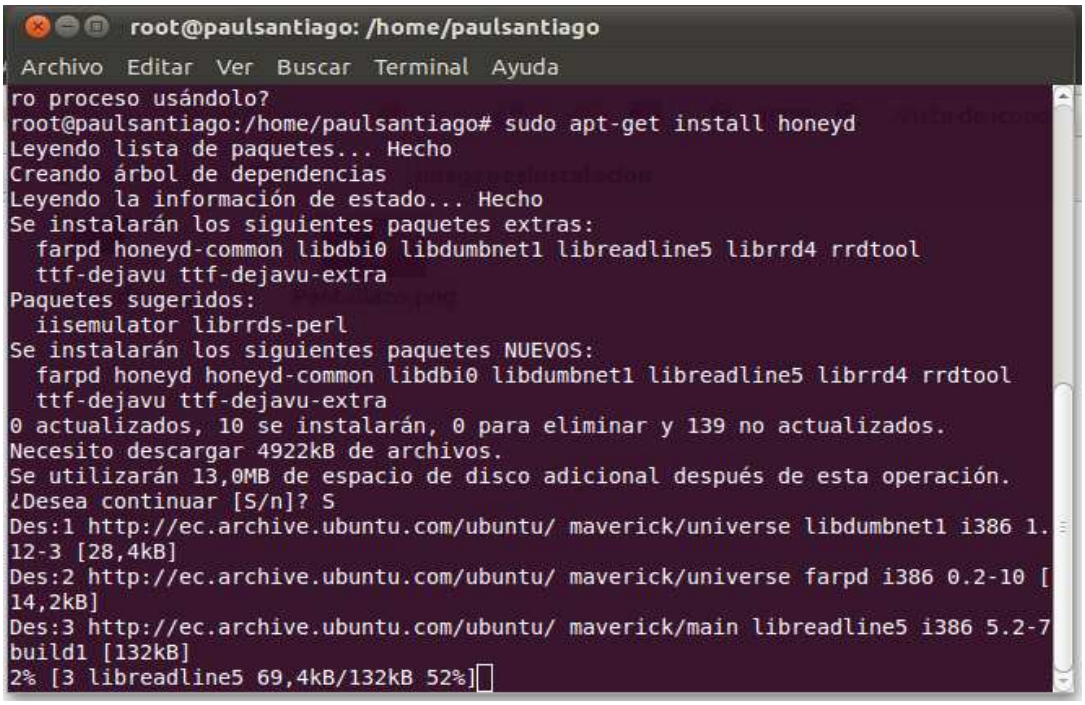

Figura IV.31. Captura de instalación de librerías honeyd

4.5. Configuración de Honeyd

La configuración de Honeyd se encuentra en el directorio /honeypot/archivos esto es en nuestro caso por lo general se encuentra en el directorio /etc/honeypot bajo el archivo honeyd.conf, se lo edita utilizando cualquier editor de texto con el siguiente comando:

root@usuario:/home/usuario# sudo nano /etc/honeypot/honeyd.conf

4.5.1. Archivo de configuración

Como es típico en un sistema Linux la configuración de los servicios se realiza por medio de edición de archivos la ubicación de los archivos a editar en nuestro caso es en la siguiente ruta:

/honeypot/archivos/honeyd.conf

Este archivo de configuración puede ser personalizado o cambiado según las necesidades de la institución u organización.

El siguiente es el archivo de configuración que se utilizará para la implementación de Honeyd en la cual podemos simular hasta 65000 sistemas operativos virtuales con los que los atacantes podrán interactuar pensando que están atacando a un servidor real. Para ello se va a explicar paso a paso cada parte del archivo de configuración de Honeyd:

Para poder crear el sistema operativo que va a ser simulado lo vamos a hacer en el mismo archivo de configuración en la ruta mencionada anteriormente para ello se explicara las operaciones realizadas dentro del archivo:

- **create.-** Este comando más un identificador cualquiera es el encargado de darle una identificación a nuestro servidor virtual.

- **set default personality "Microsoft Windows XP Home Edition".-** Mediante está línea de comando se va a asignar la personalidad del sistema operativo virtual que va a ser simulado en este caso van a ser los 3 sistemas

mencionados anteriormente como son Windows XP, Suse 8.0 y Microsoft Windows 2000 Server SP3.

- **set default tcp action.-** Con este comando el administrador de la red puede abrir, resetear, bloquear los protocolos con el fin de tratar de poner mayor obstáculo a los atacantes, únicamente ubicando luego del comando las palabras open, reset y block respectivamente.

- **add default tcp port.-** Añadimos además al archivo de configuración está línea de comando, la cual va a simular la interacción con el atacante. Al agregar por ejemplo el protocolo tcp mediante el puerto 80, el atacante va a poder interactuar como si fuera un http.

- **"perl /honeypot/archivos/scripts/win32/".-** Se debe agregar además la ruta donde se encuentran almacenados los scripts que simularan los servicios para la conexión como por ejemplo telnetd.sh, web.sh, ftp.sh, etc.

- **bind 192.168.1.130 win2k.-** Es la dirección IP en la cual va a tomar el sistema operativo virtual, tal como si fuera la dirección de un equipo dentro de la red.

4.5.2. Simulación de servicios

Una vez que se tiene listo el archivo de configuración de honeyd, el comportamiento de los puertos se resume en lo siguiente:

Puerto TCP

- **Open:** Responde con un Syn/Ack si la conexión se establece
- **Block:** Pérdida de los paquetes y no responde
- **Reset:** Responde con un RST
- **Tarpit:** añadiendo con

Puerto UDP

- **Open:** NO responde
- **Block:** Pérdida de los paquetes y no responde
- **Reset:** Responde con un puerto ICMP con mensaje de error

Puerto ICMP

- **Open:** Respuesta a los paquetes ICMP
- **Block:** Pérdida de los paquetes y no responde

Luego de realizar el archivo de configuración empieza la simulación de los intrusos con el sistema Honeyd trampa. Para mejorar el sistema es necesario también cambiar los scripts en los cuales va a simular protocolos de red, páginas web etc

Archivo de configuración de ejemplo:

Script de simulación Telnet:

```
#!/bin/sh
#
. scripts/misc/base.sh

SRCIP=$1
SRCPORT=$2
DSTIP=$3
```

```
DSTPORT=$4

SERVICE="telnet"
HOST="serv"

state="login"
count=1

my_start

login_failed() {
sleep 3
echo "Login incorrecto"
if [ $count -eq 4 ]; then
        my_stop
fi
count=$[$count+1]
state="login"

echo ""
echo -n "$HOST Login: "

}

echo "Bienvenido a SuSE Linux 7.0 ESPOCH-ECUADOR"
echo -n "$HOST Login: "


while read name; do

# remove control-characters
name=`echo $name | sed s/[[:cntrl:]]//g`

echo "$name" >> $LOG
```

```
case $state in
login)
        if [ -z $name ]; then
            login_failed
        else
            state="pass"
            echo -n "Password: "
        fi
;;
pass)
        login_failed
;;
esac

done
my_stop
```

4.5.3. Contenido del archivo de configuración honeyd.conf

Lo que se muestra a continuación es el archivo completo de configuración del honeypot, aquí es en donde se aplica todo lo visto anteriormente para lograr la simulación de los equipos utilizando sus respectivas personalidades.

```
#####  Configuración Honeyd #####
# Last Updated: 2010-2011

#########################################################################
### Aqui vamos a iniciar con las plantillas predeterminadas           ###
### Comportamiento a una dirección IP                                 ###
### Plantilla por defecto y poner el nombre                           ###
###                                                                   ###
#########################################################################

### Default Template
create default
```

```
# Set default behavior
set default personality "Microsoft Windows XP Home Edition"
set default default tcp action reset
set default default udp action reset
set default default icmp action open
add default tcp port 21 "perl /honeypot/archivos/scripts/win32/msftp.sh "
add default tcp port 22 "sh /honeypot/archivos/scripts/unix/linux/win32/ssh.sh $ipsrc $sport $ipdst $dport"
add default tcp port 23 "sh /honeypot/archivos/scripts/unix/linux/win32/telnetd.sh $ipsrc $sport $ipdst $dport"
add default tcp port 80 "sh /honeypot/archivos/scripts/unix/linux/win32/apache.sh $ipsrc $sport $ipdst $dport"

add default tcp port 139 open
add default tcp port 137 open
add default udp port 137 open
add default udp port 135 open

### Standard Windows 2000 computer
create win2k
set win2k personality "Microsoft Windows 2000 Server SP3"
set win2k default tcp action open
set win2k default udp action open
set win2k default icmp action open
set win2k uptime 3567
set win2k droprate in 13
add win2k tcp port 21 "sh /honeypot/archivos/scripts/win32/win2k/msftp.sh $ipsrc $sport $ipdst $dport"
add win2k tcp port 23 "sh /honeypot/archivos/scripts/win32/win2k/telned.sh $ipsrc $sport $ipdst $dport"
add win2k tcp port 80 "sh /honeypot/archivos/scripts/win32/win2k/iis.sh $ipsrc $sport $ipdst $dport"
add suse80 tcp port 21 "sh /honeypot/archivos/scripts/unix/linux/suse8.0/proftpd.sh $ipsrc $sport $ipdst $dport"
bind 192.168.1.130 win2k

### Linux Suse 8.0 template
create suse80
set suse80 personality "Linux 2.4.7 (X86)"
```

set suse80 default tcp action open
set suse80 default udp action open
set suse80 default icmp action open
set suse80 uptime 79239
set suse80 droprate in 4
add suse80 tcp port 21 "sh /honeypot/archivos/scripts/unix/linux/suse8.0/proftpd.sh $ipsrc $sport $ipdst $dport"
add suse80 tcp port 22 "sh /honeypot/archivos/scripts/unix/linux/suse8.0/ssh.sh $ipsrc $sport $ipdst $dport"
add suse80 tcp port 23 "sh /honeypot/archivos/scripts/unix/linux/suse8.0/telnetd.sh $ipsrc $sport $ipdst $dport"
add suse80 tcp port 80 "sh /honeypot/archivos/scripts/unix/linux/suse8.0/apache.sh $ipsrc $sport $ipdst $dport"
bind 192.168.1.135 suse80

4.6. Interacción con Honeyd

Antes de poner a trabajar a Honeyd se puede decir que este interactúa con algunas aplicaciones para su mejor funcionamiento.

Nmap es una aplicación multiplataforma usada para explorar redes y obtener información acerca de los servicios, sistemas operativos y vulnerabilidades derivadas de la conjunción de éstos.

Es muy usado por todo aquél que se interesa por las tareas de seguridad y hacking en general, desde Administradores de Sistemas a interesados con fines menos respetables. Las técnicas de escaneo que usa Nmap han sido ya implementadas en sistemas de detección de intrusos y firewalls, ya que los desarrolladores de sistemas de seguridad también usan Nmap en su trabajo y toman medidas.
No obstante, pese a estar ampliamente documentado su funcionamiento, hay formas de escaneo que lo hacen difícil de detectar cuando se trata de obtener información. Para la instalación de nmap en Ubuntu es suficiente ejecutar el siguiente comando:

root@usuario:/home/usuario# apt-get install nmap

Ahora se debe probar el funcionamiento de nmap, para ello hay que verificar si se encuentran corriendo los sistemas abiertos, realizamos el escaneo con el siguiente comando:

root@usuario:/home/usuario# nmap 192.168.1.0/24

Hay varios estados posibles para un puerto como ya se dijo. Si hay algún servicio escuchando en él, el estado es OPEN. Si no hay servicios en ese puerto puede responder con un mensaje ICMP o simplemente con nada.

Con el siguiente comando añadimos las rutas:

root@usuario:/home/usuario# sudo route -n add –net 192.168.1.0/24 gw 192.168.1.1

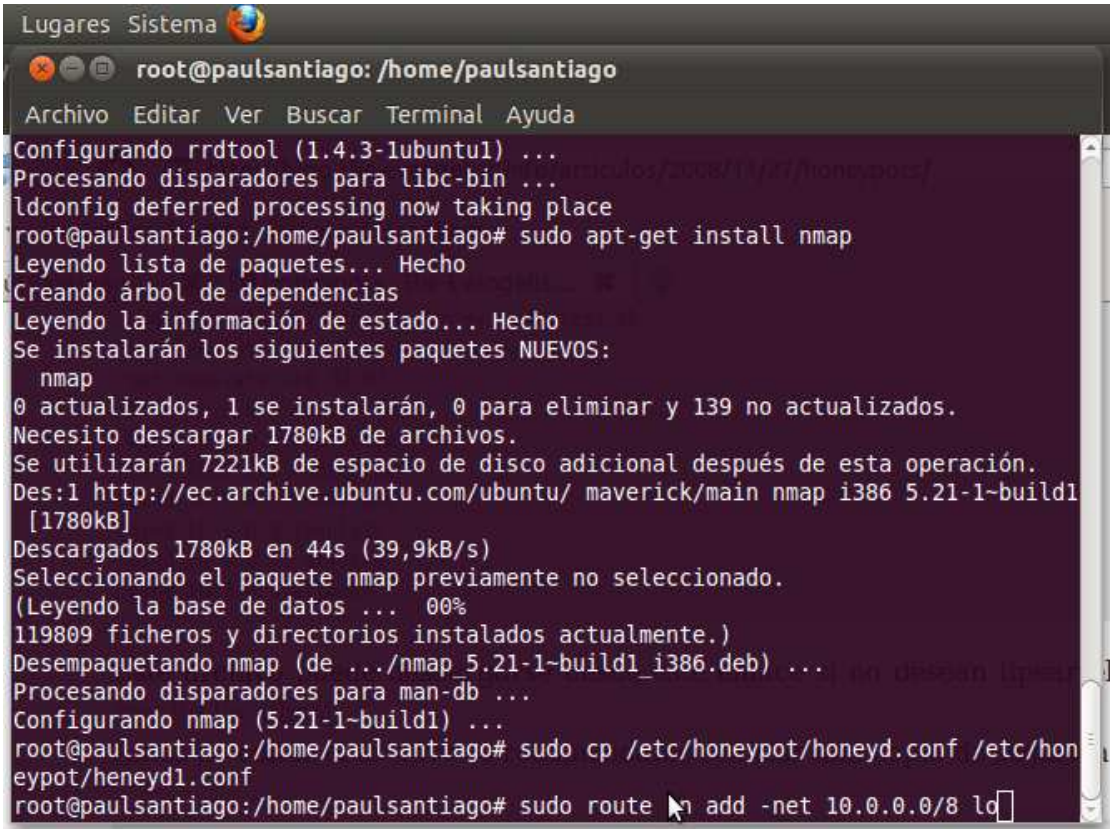

Figura IV.32. Comando route-add

4.6.1. Arranque Honeyd

Ahora si iniciaremos el demonio Honeyd para que los atacantes interactúan con nuestros servicios virtuales para ello hay que ejecutar el comando:

root@usuario:/home/usuario# honeyd -f honeyd.conf -p nmap.prints -x xprobe2.conf -a nmap.assoc -0 pf.os -l /var/log/honeyd 192.168.1.100-192.168.1.253

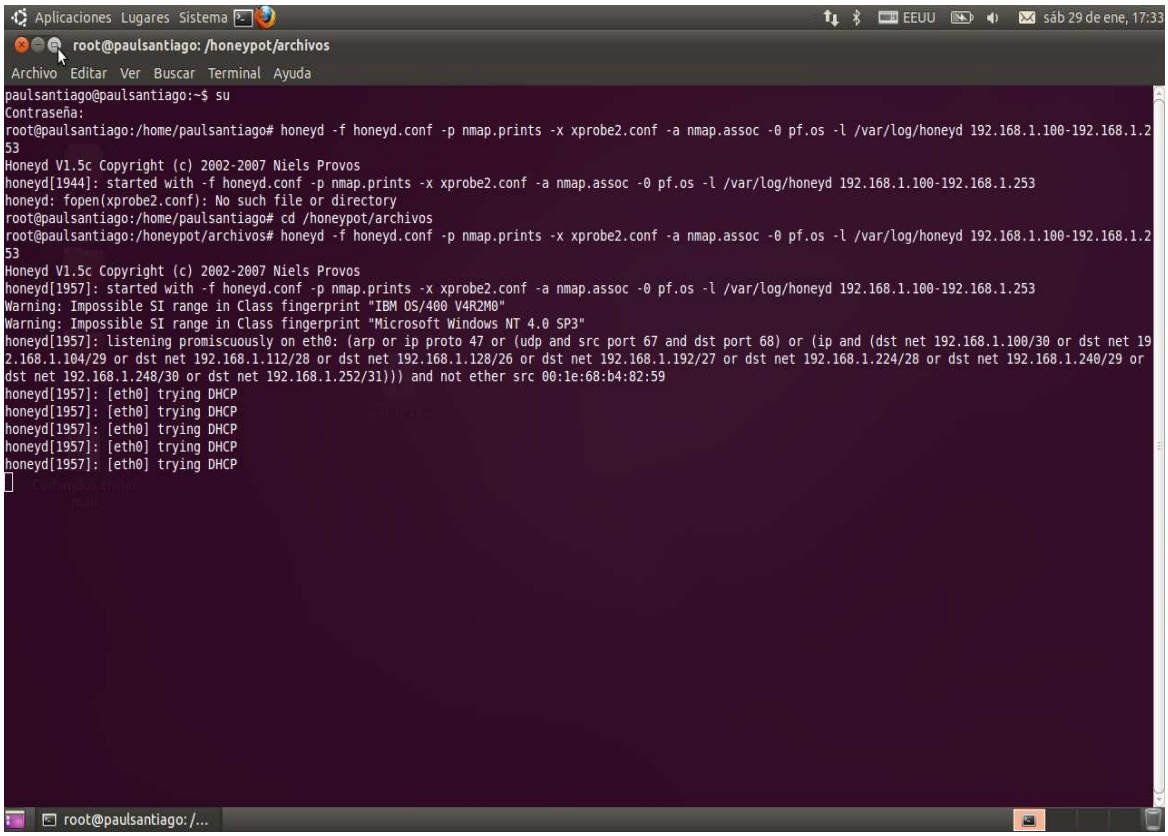

Figura IV.33. Inicio de Honeyd

Con este comando se ejecuta honeyd. Los parámetros -p y -f significan el uso de los archivos para las huellas y la configuración.

4.6.2. Simulación de un ataque a honeyd

4.6.2.1. Herramientas usadas para el ataque

Ipscan:

Ipscan es una herramienta que puede escanear un completo rango de direcciones IP para comprobar su disponibilidad. La herramienta muestra la dirección IP, el tiempo de respuesta. Esta herramienta utiliza la función de raw socket y el algoritmo de árbol AVL.

Free Port Scanner:

FreePortScanner es una pequeña y sencilla utilidad que tiene como función principal realizar un análisis de los puertos en las plataformas Win32.

Puede analizar los puertos en las maquinas en pocos segundos y también puede realizar análisis a intervalos predefinidos.

Tiene una interfaz sencilla y es fácil de usar.

Nessus:

Es un programa de escaneo de vulnerabilidades en diversos **sistemas operativos**. Consiste en nessusd, el daemon Nessus, que realiza el escaneo en el sistema objetivo, ynessus, el cliente (basado en consola o gráfico) que muestra el avance y reporte de los escaneos. Desde consola nessus puede ser programado para hacer escaneos programados con cron.

En operación normal, nessus comienza **escaneando los puertos** con **nmap** o con su propio escaneador de puertos para buscar puertos abiertos y después intentar varios **exploits** para atacarlo. Las pruebas de vulnerabilidad, disponibles como una larga lista de plugins, son

escritos en NASL (Nessus Attack Scrpting Language, Lenguaje de Scripting de Ataque Nessus por sus siglas en inglés), un lenguaje scripting optimizado para interacciones personalizadas en redes.

Opcionalmente, los resultados del escaneo pueden ser explotados en reportes en varios formatos, como texto plano, **XML, HTML** y **Latex.** Los resultados también pueden ser guardados en una base de conocimiento para hacer referencia en futuros escaneos de vulnerabilidades.

Algunas de las pruebas de vulnerabilidad de Nesus pueden causar que los servicios o sistemas operativos se corrompan y caigan. El usuario puede evitar esto desactivando **"unsafe test"** (pruebas no seguras) antes de escanear.

4.6.2.2. Ataque al honeypot

Escannear direcciones IP : Un atacante cuando incurre en una red primeramente busca los objetivos mas interesantes dentro de la misma, para lo cual ejecuta cualquier herramienta para detectar los equipos que se hallan en la red, en el presente ejemplo se usara la herramienta IPScan, un software muy sencillo que identifica las direcciones activas dentro de la red.

Figura IV.34. Intefaz IP Scanner

Escannear puertos: Una vez identificadas las direcciones ip se puede utilizar herramientas para descifrar que puertos tiene abierto el equipo y su protocolo en nuestro caso podemos utilizar el Free Port Scanner

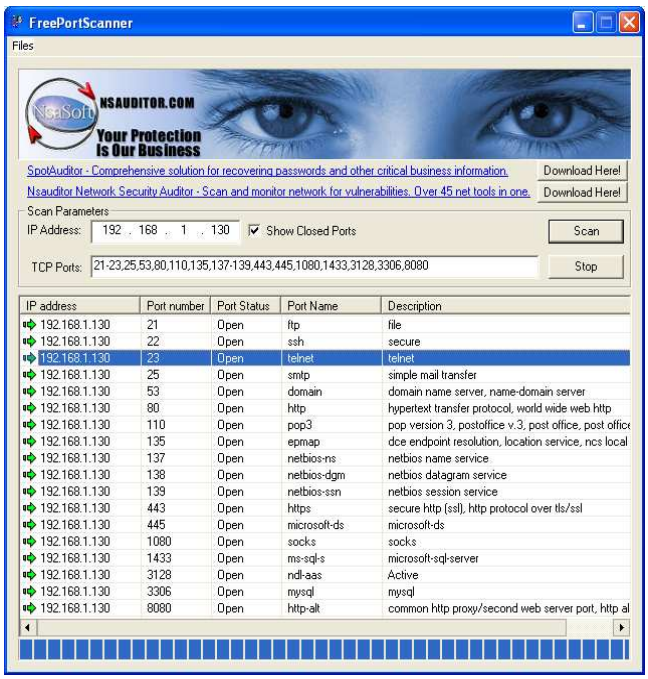

Figura IV.35. Captura Free Port Scanner

Auditor de redes: Una de las herramientas mas completas y usadas para los ataque es Nesus, para el presente caso luego de identificar las ips de los equipos de la red se utiliza este software para determinar las debilidades de los sistemas honeypot los cuales deben darnos resultados tal como si fueran sistemas reales.

A continuación se detalla una auditoría realizada con la herramienta Nessus luego de haber detectado las ip disponibles dentro de la red.

a) Instalación de Nessus

Para iniciar la auditoria se debe realizar la instalación de Nessus descargando su instalador para este caso usaremos el de Windows, el link de descarga es el http://www.nessus.org/download.

Una vez descargado el fichero se deberá realizar una típica instalación de windows, la cual cuando se haya finalizado nos instalara dos componentes un Nessus server y un Nessus client.

Para poder empezar a utilizar la herramienta debemos ingresar en Nessus server y crear un usuario, para este caso se usa el usuario honey con una clave 0000 todo esto dentro de Manage Users.

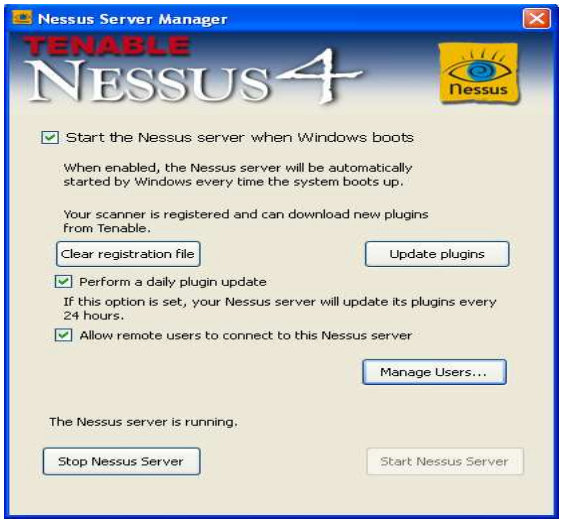

Figura IV.36. Intefaz Nessus Server

b) Utilización de Nessus

Una vez creado el usuario se procede a ingresar a Nessus cliente,

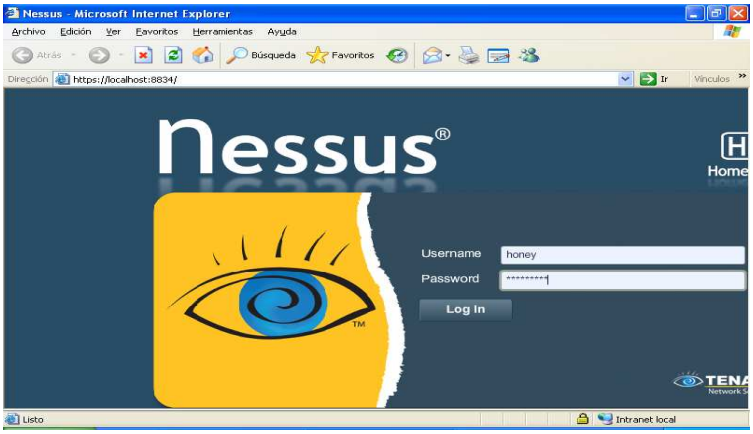

Figura IV.37. Intefaz Nessus Cliente

Inmediatamente luego de la validación se encuentra la interfaz principal de Nessus en donde se debe crear primeramente una Política de escaneo configurando varios parámetros como tipos de protocolos y puertos.

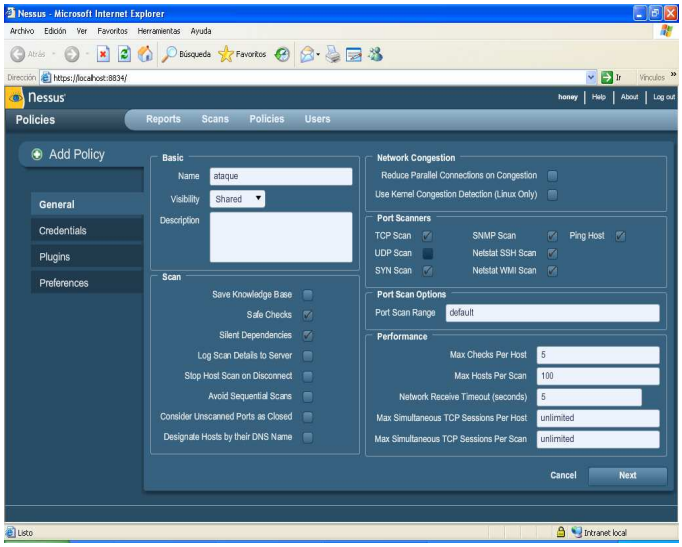

Figura IV.38. Creación de Políticas

Con las ips que se encontró habilitadas en la red se procede a crear escaneos según como se requiera, de esta manera Nessus examina el computador completo en búsqueda de debilidades y oportunidades de invasión o simplemente como medidas de seguridad para proteger la red.

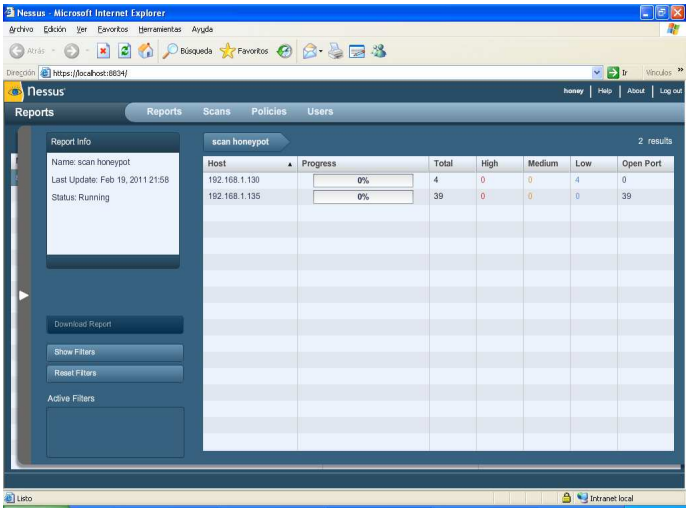

Figura IV.39. Escaneo de Equipos

c) Reporte de Nessus

Una vez terminados los escaneos se puede descargar un informe completo en formato html, el cual presenta la identificación de las debilidades, características del equipo y la posible solución para evitar la vulnerabilidad.

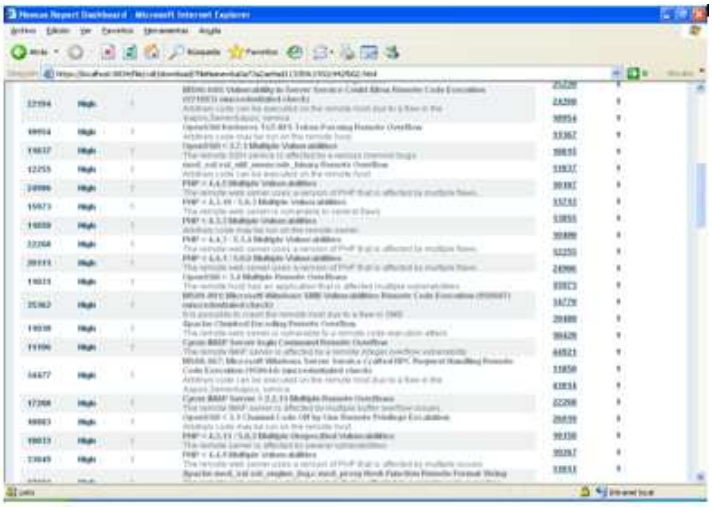

Figura IV.40. Reporte de Nessus

En el presente ejemplo se va a tomar el equipo con dirección de red 192.168.1.135 el cual fue uno de los que se encontró con el programa IPScan mediante Nessus se pudo observar que tiene el puerto telnet abierto tal y como un computador real.

A continuación se va a intentar ingresar mediante telnet por medio de la consola de Windows xp de la siguiente manera.

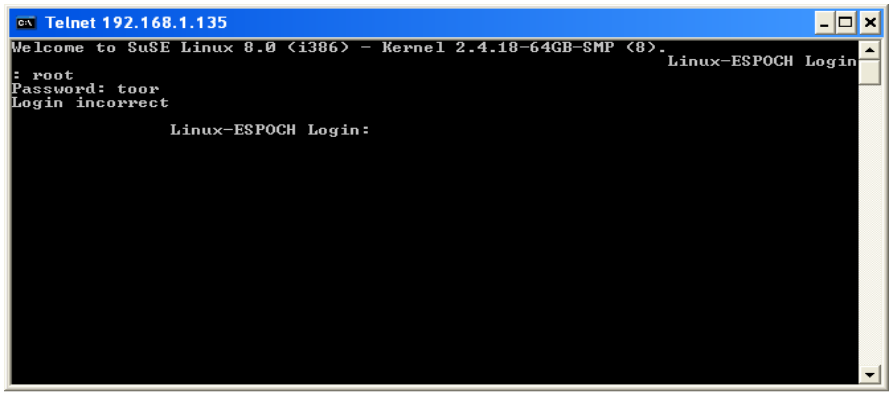

Figura IV.40. Intento de Ingreso mediante Telnet

Se puede observar que el honeypot muestra una interfaz que cualquier invasor va a verla como real intentando ingresar y descifrar las claves, las cuales van siendo registradas en los archivos log del honeyd.

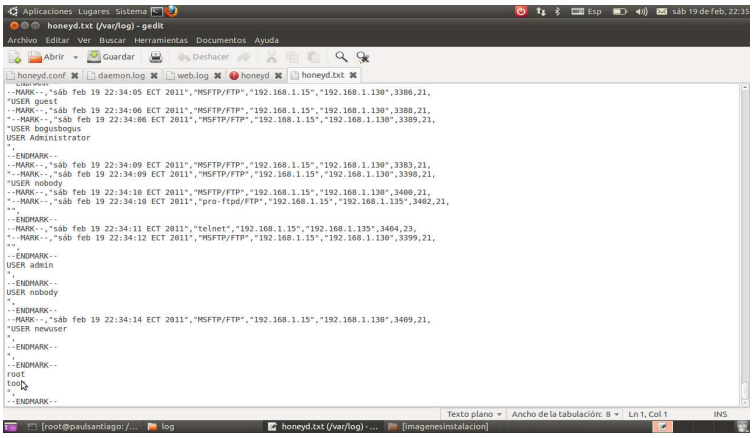

Figura IV.41. Captura de sucesos honeyd

Resultados de Ataque: Mientras las herramientas de invasión actúan honeyd va entregándoles respuestas como si fuera un computador real y ademas capturando todo cuanto recibe del atacante.

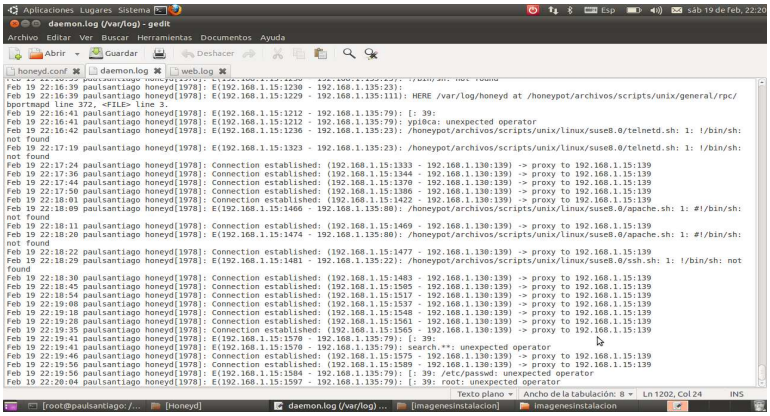

Figura IV.42. Reporte honeyd

Como se puede observar en los resultados es muy difícil que el atacante pueda darse cuenta que está jugando con un computador simulado,

Esta es una pequeña muestra de las vulnerabilidades que se pudo encontrar con las herramientas para escaneo, de la misma manera se encontró puertos ftp, http, ssh abiertos y vulnerables. Pero al mismo tiempo mientras el atacante confía estar descifrando las debilidades de su víctima está jugando dentro del sistema virtual creado para disuadirlo y entretenerlo dejando de lado los sistemas reales.

4.7. Análisis de los registros de un ataque a honeyd

Los sistemas Honeyd almacenan todas las actividades generadas por el atacante en contra de honeyd, la ruta donde se almacenan los registros es: /var/log donde se encuentran los siguientes archivos:

- Daemon.log
- Honeyd.txt
- Syslog

Así se muestra un ejemplo del archivo honeyd.txt

--MARK--,"lun nov 2 17:04:26 ECT
2009","telnet","192.168.1.30","192.168.1.135",32842,23,
"",
--ENDMARK--
",
--ENDMARK--
--MARK--,"lun nov 2 17:05:05 ECT
2009","telnet","192.168.1.30","192.168.1.135",32850,23,
"",
--ENDMARK--
--MARK--,"Vie dic 10 17:05:25 ECT
2009","telnet","192.168.1.20","192.168.1.135",1196,23,
"",
--ENDMARK--
--MARK--,"Sab dic 11 17:05:57 ECT
2009","telnet","192.168.1.20","192.168.1.135",1197,23,
"",
--ENDMARK--
--MARK--,"lun ene 7 17:14:20 ECT
2009","telnet","192.168.1.30","192.168.1.135",32963,23,
" !"'#" 'hacker
password ",
--ENDMARK--
--MARK--,"lun ene 27 17:25:09 ECT
2009","ssh","192.168.1.20","192.168.1.135",1270,22,
"SSH-2.0-PuTTY_Release_0.60
",
--ENDMARK--
",
--ENDMARK--
--MARK--,"lun nov 2 17:48:27 ECT
2009","telnet","192.168.1.20","192.168.1.135",1362,23,
" 'hacker
password

En los logs generados por el Honeyd cuando interactúan con los atacantes se puede observar el día, la fecha y la hora en la que intento ingresar el atacante, el protocolo que utilizaron, la dirección ip del atacante, la dirección IP de la máquina simulada a la que están atacando y si teclearon algún usuario y contraseña también se registra.

4.7.1. Herramienta Logwatch

Logwatch es un analizador de logs modular que se ejecuta cada noche y envía a correos electrónicos los resultados de estos análisis. También se puede ejecutar desde la salida del comando line. La salida del servicio se puede limitar en particular. Los subíndices que son responsables de la salida, sobre todo convertir las líneas de registro sin procesar en formato estructurado.

Logwatch generalmente ignora el componente de hora en la salida, es decir, usted sabrá que el caso reportado se registró en el intervalo de tiempo necesario, pero se tendrá que ir a los archivos de registro sin procesar para obtener más detalles.
Para instalar Logwatch conjuntamente con todos los requerimientos y librerías se ejecuta el siguiente comando:

sudo apt-get install logwatch.

4.7.2. Configuración Logwatch

En primer lugar se necesita asegurar de que el servidor es capaz de enviar los correos fuera para ello se puede hacer esto usando postfix con la configuración del servidor SMTP
Luego de la instalación se procede a editar el archivo logwatch.conf el cual contiene la configuración de los parámetros necesarios para el funcionamiento de la herramienta.

sudo nano /usr/share/logwatch/default.conf/logwatch.conf

Dentro del archivo de configuración se deben editar las siguientes opciones:

- Output = mail
- Format = html
- MailTo = test@gmail.com

CONCLUSIONES

- Mediante la utilización de parámetros e indicadores se ha logrado ejecutar el análisis comparativo de las herramientas de Administración para la detección de intrusiones en la red, Honeyd, BOF y Specter concluyendo que la herramienta más idónea para implantar la aplicación es Honeyd.
- La instalación e implementación de una herramienta de detección de intrusiones en la red está brindando mayor seguridad y confiabilidad al usuario al momento de crear sus sistemas operativos virtuales.
- En instalación de las herramientas de detección de intrusiones en la red los honeypots Honeyd, BOF y Specter se puede concluir que la herramienta Honeyd posee un mejor rendimiento en lo referente a instalación.
- Se utilizo la distribución Ubuntu para la instalación del Honeypot Honeyd pues es más fácil de usar y se lo puede utilizar en forma privada, pública o comercial sin tener que pagar.
- Se concluye que la herramienta Honeyd tiene un mayor grado de funcionalidad ya que presenta muchas formas para la generación de sistemas operativos virtuales personalizados, mayor documentación y ayuda que las demás.
- En lo referente al Soporte Técnico oficial en línea se puede concluir que la herramienta Honeyd tiene una extensa información organizada no solo de sus librerías, sino de conceptos teóricos que ayudan a la mejor comprensión del funcionamiento de la herramienta Honeypot.
- Luego de estudiar los conceptos básicos sobre las herramientas de detección de intrusiones en la red se puede concluir que la herramienta Honeypot Honeyd maneja muchos sistemas operativos virtuales que son aplicables en tiempo real e inteactúa mejor que las otras herramientas con el intruso.

- Se ha concluido que los Honeypots pueden ser utilizados con el fin de prevenir detectar o responder a los ataques, lo cual va a ayudar a los administradores para la investigación y recopilación de la información de las amenazas para poder entender y defenderse de los atacantes.

RECOMENDACIONES

- Para lograr un correcto funcionamiento de honeyd, se recomienda su implementación dentro de la DMZ, inmediatamente luego del firewall y fuera de la red real, esto con el fin de lograr el registro de atacantes desde el internet los cuales han logrado sobrepasar el firewall y ataques dentro de la rede interna, esto evitará también el número de falsos positivos.

- Al asignar un nombre a las personalidades de los equipos simulados se debe evitar poner a las máquinas nombres como “honeypot”, “attack-me” o de la misma forma evitar nombres que delaten el objetivo del honeypot, mismo que debe pasar desapercibido y simular lo mejor que se pueda un sistema real.

- El momento de reservar las direcciones ip mediante el comando para la inicialización de honeyd, se deberá tomar en cuenta que el rango preestablecido de direcciones no se encuentre dentro de la red real, ya que puede ocasionar conflicto con otros equipos.

- Se recomienda usar honeyd sobre sistemas GNU, ya que son sistemas más seguros y menos propensos a que los intrusos se apropien de esta máquina y la usen como herramienta para el ingreso a la red real.

RESUMEN

Investigación que tiene como objetivo estudiar y analizar comparativamente herramientas de detección de intrusiones en la red mediante Honeypots como Honeyd, Specter y BackOfficer Friendly. La herramienta seleccionada se implementara en el Departamento de Sistemas y Telematica de la ESPOCH, permitiendo conocer de mejor manera el comportamiento de los intrusos y de esta forma tomar medidas pro-activas de seguridad.

En la ejecución del análisis comparativo se determinaron y se describieron los siguientes parámetros : instalación, seguridad, funcionalidad, portabilidad, soporte técnico y situación legal, con sus respectivos indicadores. Mediante estadística descriptiva y, utilizando el método Chi cuadrado se realizó la representación en un diagrama de barras simple de la sumatoria obtenida de la tabulación de todos los parámetros, determinándose que la herramienta más idónea para implantar un servidor seguro es la herramienta Honeyd que alcanzó un porcentaje de 95.29% seguido de la herramienta Specter con un 65.88% y la herramienta BackOfficer Friendly con un 64.70%.

Para la implementación del honeypot se utilizó el sistema operativo Ubuntu 10.10 en el cual se configuró la herramienta simulando sistemas microsoft y linux con los protocolos mas comunes habilitados como el SSH, Telnet, FTP, HTTP entre otros. Con un computador instalado microsoft windows Xp se procedió a realizar ataques con diferentes herramientas, observando y analizando los resultados reflejados en los archivos de almacenamiento de logs.

Para lograr mejores resultados en la implementación de la herramienta honeyd se recomienda hacerlo en la zona desmilitarizada de la ESPOCH para evitar falsos positivos y falsos negativos.

SUMARY

The objectives of this research are to estudy and analize comparatively, intrusions and detection tools in the network using Honeypots like Honeyd, Specter y BackOfficer Friendly. The selected tool will be implemented in the Telematic and systems department of ESPOCH, allowing knowing the behavior of the intrusions and taking pro-active security decisions.

Putting in practice the comparative analysis was determined and described the next parameters: Installation, security, functionality, portability, technical support and legal situation with their respective indicators. Thru descriptive statistics and using the Chi square method was developed a representation of a diagram of simple bars of the sum that we got on the parameters tabulation, setting that the best tool o implant a save server, is the Honeyd tool that reached a 95.29 % followed by Specter tool with 65.88 % and the BackOfficer Friendly with a 64.70 %.

To implement the honeypot was used the Ubuntu 10.10 operation system, in which was set up the tool simulating Microsoft and linux systems with the most commons protocols like SSH, Telnet, FTP, HTTP, and others. With a Microsoft windows xp installed in a computer, we proceeded to attack with different tools observing and analyzing the results in the logs storage archives.

To achieve better results in the implementation of the Honeyd tool we recommended doing it in the demilitarized zone of the ESPOCH to avoid false positives and false negatives.

GLOSARIO DE TERMINOS

ARP.- Protocolo que emplea una computadora para correlacionar una dirección IP con una dirección de hardware.

Back Officer Friendly.- Friendly es una aplicación de servidor de suplantación de identidad que se ejecuta en el sistema Windows o UNIX, y te avisa cada vez que alguien intenta el control remoto del sistema mediante Back Orifice.

Back Orifice.- Es un programa de control remoto de ordenadores que funciona bajo un servidor y un cliente. Si colocamos el servidor a otro ordenador remoto, es posible desde el cliente, gobernar cualquier función del ordenador remoto.

Honeyd.- Honeyd es un honeypot.- Un honeypot simula redes con hosts activos con puertos y servicios abiertos, entonces se tienen redes simuladas levantadas para atraer atacantes a dichas redes.

Honeypots.- Software o conjunto de computadores cuya intención es atraer a atacantes, simulando ser sistemas vulnerables o débiles a los ataques. Es una herramienta de seguridad informática utilizada para recoger información sobre los atacantes y sus técnicas. se limitan a simular sistemas operativos no existentes en la realidad y se les conoce como honeypots de baja interacción y son usados fundamentalmente como medida de seguridad.

IDS.- Sistema que detecta manipulaciones no deseadas, especialmente a través de la red, para detectar tráficos de esta y el uso malicioso de la computadora.

IP.- Protocolo para la comunicación en una red a través de paquetes conmutados, los datos se envían en forma de bloques de determinados tamaños.

Licencias.- Es una especie de contrato, en donde se especifican todas las normas y clausulas que rigen el uso de un determinado programa, principalmente se estipulan los alcances de uso, instalación, reproducción y copia de estos productos.

Logs.- Archivo o grupo de archivos que contienen una lista de cada archivo que fue accedido, en general se almacena la dirección IP la fecha y hora de acceso, el navegador o agente usado etc.

Nmap.- Es una de las herramientas más comunes utilizadas para determinar el tipo de sistema operativo.

Open Source.- Denominación para aquellas aplicaciones que tienen su código fuente liberado. Los programas de código abierto suelen ser libres.

Seguridad informática.- Es una disciplina que relaciona a diversas técnicas, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información.

Specter.- Es un honeypot de baja interacción emula una variedad de servicios. Honeypots en la detección, alerta y recogida de información

Falsos positivos.- Se trata de un registro o alarma generada cuando no existe ataque un ataque real.

Falsos negativos.- Es la omisión de alarma cuando hay verdaderamente un ataque.

BIBLIOGRAFÍA

1.- A REVIEW OF *HONEYPOTS: TRACKING HACKERS* BY LANCE SPITZNER
http://www.associatedcontent.com/article/344024/a_review_of_honeypots_tracking_hackers.html
2010/12/15

2.- A VIRTUAL HONEYPOT FRAMEWORK
http://www.citi.umich.edu/u/provos/honeyd/
2010/11/09

3.- BACK ORIFICE
http://www.cultdeadcow.com/tools/bo.html
2010/11/02

4.- CERT WARNING FOR BACK ORIFICE SCANS
http://www.cert.org/summaries/CS-98-08.html
2010/11/09

5.- CLIENT HONEYPOT
http://en.wikipedia.org/wiki/Client_honeypot
2010/11/17

6.- DEFINITION SPECTER
http://www.specter.ch/introduction50.htm
201012/12

7.- DEVELOPMENTS OF THE HONEYD VIRTUAL HONEYPOT
http://www.honeyd.org
2010/11/09

8.- DEPLOYING HONEYPOTS WITH HONEYD
http://ulissesaraujo.wordpress.com/2008/12/08/deploying-honeypots-with-honeyd/
2010/11/08

9.- HONEYD AND ARPD
http://www.citi.umich.edu/u/provos/honeyd/
2010/11/16

10.- HONEYPOTS
http://biblioteca.utec.edu.sv/siab/virtual/articulos_soft_libre/Honeypots.pdf
2010/12/17

11.- HONEYPOTS MODELOS Y PROCESOS DE ANÁLISIS DE DATOS COLECTADOS POR SENSORES
http://www.cert.uy/historico/pdf/GSI_Honey.pdf
2010/11/24

12.- HONEYPOTS Y HONEYNETS
http://el-directorio.org/Seguridad/Honeypots
2010/11/20

13.- INSTALACIÓN Y CONFIGURACIÓN DE UNA HONEYPOT
http://sistemasdedecepcion.blogspot.com/2008_06_01_archive.html
2010/01/16

14.- PROVOS, N.and HOLZ, T. (2007). *Virtual* Honeypots: from botnet tracking to intrusion Detection. Boston – EEUU, Addison-Wesley. PP. 180-220, 240-270

15.- QUALITY TESTING, HONEYD
http://www.quality-testing.com/honeyd-parte-i-configuracion
2010/11/01

16.- SISTEMA DE DETECCIÓN DE INTRUSOS
http://es.wikipedia.org/wiki/Sistema_de_detecci%C3%B3n_de_intrusos
2011/01/10

17.- SISTEMA DE DETECCIÓN DE INTRUSOS
http://ohem.wordpress.com/2009/07/17/sistema-de-deteccion-de-intrusos/
2010/07/17

18.- SPITZNER Lance. (2002). Honeypots: tracking hackers. Boston – EEUU, Addison-Wesley. PP. 20-150.

19.- WORM ACTIVITY
http://research.arbor.net/up_media/up_files/snapshot_worm_activity.pdf
2010/10/11