UNIVERSIDAD TECNICA DE COTOPAXI

CARRERA DE CIENCIAS DE LA INGENIERIA Y APLICADAS

TESIS DE GRADO PREVIO A LA OBTENCION DEL TITULO DE INGENIERIA EN INFORMATICA Y SISTEMAS COMPUTACIONALES

TEMA:

"DESARROLLO DE PRUEBAS DE UN HONEYPOTS (SERVIDOR TRAMPA) PARA DETECCIÓN DE INTRUSOS"

POSTULANTES:

Molina Castellano Mayra Lili

Tapia Toctaguano Alexandra Verónica

DIRECTOR:

Ing. Patricio Navas

Latacunga 26 de Junio del 2008

AUTORIA

Nosotros: Molina Castellano Mayra Lilí y Tapia Toctaguano Alexandra Verónica declaramos que el trabajo de investigación aquí presentado es de nuestra autoría: que no ha sido previamente presentado, y que hemos consultado todo lo que en este tomo está incluido.

Molina Castellano Mayra Lilí

C.I. 050283198-5

Tapia Toctaguano Alexandra Verónica

C.I. 050234611-7

CERTIFICACION

HONORABLE CONSEJO ACADEMICO DE LA UNIVERSIDAD TECNICA DE COTOPAXI

De mi consideración.

Cumpliendo con lo estipulado en el capitulo IV, (art. 9 literal f), del reglamento del curso profesional de la Universidad Técnica de Cotopaxi, informo que las postulantes: Molina Castellano Mayra Lilí y Tapia Toctaguano Alexandra Verónica, han desarrollado su tesis de grado de acuerdo al planeamiento formulado en el plan de tesis con el Tema: "DESARROLLO DE PRUEBAS DE UN HONEYPOTS (SERVIDOR TRAMPA) PARA DETECCIÓN DE INTRUSOS", cumpliendo con los objetivos planteados.

En virtud de lo antes expuesto, considero que la presente tesis se encuentra habilitada para presentarse al acto de la defensa de tesis.

Latacunga, 28 de Mayo del 2008

Atentamente,

Ing. Patricio Navas

DIRECTOR DE TESIS

CERTIFICACION DE TRADUCCION

Yo, Sonia Jimena Castro Bungacho, portadora de la Cedula de Identidad Nº 050197472-9 en calidad de Docente del Idioma de Ingles de la Universidad Técnica de Cotopaxi, tengo a bien Certificar: que las postulantes: Molina Castellano Mayra Lilí con C.I 050283198-5 y Tapia Toctaguano Alexandra Verónica con C.I 050234611-7, han realizado la debida corrección del summary de la Tesis de Grado con el Tema: "DESARROLLO DE PRUEBAS DE UN HONEYPOTS (SERVIDOR TRAMPA) PARA DETECCIÓN DE INTRUSOS", el cual se encuentra bien estructurado por lo que doy fe del presente trabajo.

Por tal motivo faculto a los peticionarios hacer uso del presente certificado como a bien lo considere.

Latacunga, 27 de Mayo del 2008

Atentamente,

Lic. Sonia Castro

Docente del Idioma de Ingles de la Universidad Técnica de Cotopaxi

AGRADECIMENTO

A Dios ante todo y a la Virgen María porque ellos siempre han estado con nosotros en nuestro corazón guiándonos por el buen camino.

A nuestros padres y familia pilares fundamentales quienes con su dedicación y ayuda hacia nosotros supieron comprendernos, apoyarnos afectiva y económicamente para la terminación del presente proyecto y la culminación de nuestra meta estudiantil.

A esta querida institución que por intermedio de sus docentes nos han guiado y entregado sabios conocimientos brindándonos la oportunidad de prepararnos para ser unas profesionales de servicio a la sociedad.

Un especial agradecimiento a nuestro director de tesis Ing. Patricio Navas por ser un actor principal de este trabajo quien con su exigencia, esfuerzo, tiempo y dedicación nos ha orientado hasta llegar a la obtención del titulo que anhelamos.

Gracias a todos

Lilì, Alexandra

DEDICATORIA

Este trabajo lo dedico a mis padres Jorge y Soledad quienes me apoyaron económicamente y moralmente en todo momento, a mi hijo Fabián Vinicio por ser la persona quien me dio aliento y fuerza para concluir con lo presente y finalmente a mis hermanos Michael, Brayan y David.

Alexandra

A mi hijo Matías Sebastián quien con su ternura me inspira a superarme día a día, a mi papa Nelson y a mi mama Mercedes quienes siempre me apoyaron y estuvieron conmigo en todos los momentos de mi vida; a mi esposo Rolando que ha sabido brindarme comprensión y apoyo diario, y finalmente a mis hermanos Edison, Cristian y Monserath que de alguna manera me ayudaron.

Lilì

INDICE GENERAL

SISTEMA OPERATIVO LINUX

CONCLUSIONES Y RECOMENDACIONES

RESUMEN

Este trabajo de investigación trata del análisis de los honeypots que tienen sus ventajas e inconvenientes. Su mayor utilidad radica en su simpleza. Al ser un mecanismo cuyo único fin consiste en que intenten abusar de él, no realiza ningún servicio real, y el tráfico que transita a través de él va a ser muy pequeño.

Si se detecta tráfico que va o viene hacia el sistema, casi con toda probabilidad va a ser una prueba, escaneo o ataque. El tráfico registrado en un sistema de este tipo es sospechoso por naturaleza, por lo que su gestión y estudio se simplifica en gran medida. Aunque, por supuesto, ocurran "falsos positivos", expresión que, en este caso, invierte su significado. Si un falso positivo se produce normalmente cuando una actividad sospechosa tomada como ataque no resulta serlo, en el ambiente de los "tarros de miel", el falso positivo sería el tráfico gestionado por la máquina que no representa una amenaza. En esta simpleza de uso de tráfico y recursos, radica su mayor ventaja. En resumen, poca información, pero muy valiosa.

Entre los problemas que puede causar, destaca la posibilidad de que se vuelva en nuestra contra. Si no se diseña de una manera absolutamente estudiada, si no se ata cada cabo, el pirata puede acabar llevándose el cebo sin ser atrapado por la caña. Si descubre alguna otra vulnerabilidad no

prevista o consigue burlar los sistemas de registro, puede usar el ordenador atacado como plataforma para otros ataques o, lo que representaría un completo fracaso del sistema, comprometer máquinas reales con datos valiosos conectados al honeypot.

SUMMARY

This investigation work is about the analysis of the honeypots that have its advantages and inconveniences. Their biggest utility resides in its simplicity. To the being a mechanism whose only end consists in that you/they try to abuse of him, doesn't carry out any real service, and the traffic that traffics through him it will be very small.

If traffic is detected that he/she goes or he/she comes toward the system, almost with all probability it will be a test, escaneo or attack. The traffic registered in a system of this type is suspicious by nature, for that that its administration and study is simplified in great measure. Although, of course, happen "false positive", expression that, in this case, it invests their meaning. If a positive reinforcement usually takes place when a suspicious activity taken as attack doesn't turn out to be it, in the atmosphere of those "jars of honey", the positive reinforcement would be the traffic negotiated by the machine that doesn't represent a threat. In this simplicity of traffic use and resources, their biggest advantage resides. In summary, little information, but very valuable.

Among the problems that it can cause, it highlights the possibility that he/she becomes in our against. If it is not designed in an absolutely studied way, if he/she doesn't get tied up each end, the pirate it can finish being taken the bait without being caught by the cane. If he/she discovers some

other not foreseen vulnerability or it is able to deceive the registration systems, it can use the computer attacked as platform for other attacks or, what would represent a complete failure of the system, to commit real machines with connected valuable data to the honeypot.

INTRODUCCION

En la actualidad cualquier computador interconectado al Internet es un potencial blanco de ataques de personas que buscan satisfacer su ego o en algunas ocasiones alterar o dañar la información de empresas con el único fin de causar daño o llamara la atención de la comunidad cibernauta.

Las amenazas que encontramos en Internet cada día va cambiando de foco antes se lo hacia en forma de virus y gusanos(Slammer, Codered), ahora en cambio encontramos lis mismos virus, gusanos informáticos, otros "personajes" que trabajan con herramientas buscando obtener ganancias.

Invitamos a que los nuevos egresados y graduados tomen a nuestra carrera como un reto el cual siempre nos va a servir para mejorar y ser buenos en cualquiera de los ámbitos que nos desenvolvemos.

Los Honeypots o servidores Trampa se han constituido en una herramienta poderosa y que sabiendo aprovecharlas podemos sacarle mucho, ya que con un equipo que tenga buenas prestaciones pueden ser de mucha utilidad y podemos atraer muchos usuarios maliciosos de la red identificarlos y protegernos de su posible ataque.

En términos generales un honeypot es un recurso de red cuyo valor mismo es el de ser atacado o vulnerado. Los beneficios se obtienen mediante mantener un cuidadoso monitorizado del mismo.

El objetivo de nuestro tema de estudio fue ofrecer un blanco interesante para los hackers demostrar que mediante un solo servidor se puede atraer muchos tipos de personajes que tratan de atacar y nosotros estamos prestos para poder detectarlos y atacarlos antes de que nos ataquen, esto es lo que se considera que la mejor defensa es el ataque.

De las fortalezas de nuestra investigación es el poder contar con suficiente información bibliográfica, además de que se baso íntegramente en los estándares internacionales para las configuraciones, no podemos dejar de mencionar la importante colaboración de parte del departamento de servicios informáticos así como de los docentes de la Universidad Técnica de Cotopaxi los mismos que facilitaron mucha información que todavía no se puede encontrar en libros o en el Internet.

Nuestro trabajo ha sido diseñado en tres capítulos:

El primero corresponde al conocimiento de algunos aspectos importantes de los Honeypots, HoneyNets, los IDS (Sistemas de Detección de Intrusos), IPS (Sistemas de Prevención de Intrusos), Firewall como alternativas de seguridades en las empresas.

El segundo corresponde al Trabajo de Campo es decir a las entrevistas realizadas a profesionales que conocen del tema, así como los elementos y parámetros para las implementaciones de los servidores Trampa, la instalación del sistema operativo que va a soportar al servidor.

En el Tercer Capitulo se encuentra el desarrollo y las pruebas de las distintas variantes de los honeypot, así como su factibilidad técnica, económica y operacional de la implementación.

Finalmente las conclusiones con sus respectivas recomendaciones las mismas que arrojo nuestro trabajo de investigación.

CAPITULO I

1. FUNDAMENTACIÓN TEÓRICA DE LAS MAQUINAS SEGURIDADES BASADAS EN SERVIDORES

1.1. SERVIDORES TRAMPA (HONEYPOT Y HONEYNET)

1.1.1. Introducción y Sinopsis

El papel de la tecnología del sistema de detección de intrusos basado en señuelos o "honeypots" - está evolucionando. Los honeypots, que alguna vez fueron utilizados principalmente por los investigadores como una forma de atraer a los hackers a un sistema de redes para estudiar sus movimientos y comportamiento, están adquiriendo una importancia cada vez mayor en la seguridad empresarial. En efecto, al brindar detección temprana de actividad no autorizada en las redes, los honeypots son ahora más útiles que nunca para los profesionales de seguridad de TI. Este artículo analiza el funcionamiento de los honeypots y su tecnología, que se está convirtiendo en el componente clave del sistema de capas de protección contra intrusos.

Los Honeypots son una emocionante tecnología nueva, con un enorme potencial para la comunidad informática. Los primeros conceptos fueron introducidos por primera vez por varios iconos en la seguridad informática, especialmente por Cliff Stoll en el libro "The Cuckoo's Egg" y

el trabajo de Bill Cheswick "An Evening with Berferd". Desde entonces, los honeypots han estado en una continua evolución desarrollándose en una poderosa herramienta de seguridad hoy en día. El propósito del presente trabajo es el de explicar exactamente qué son los honeypots, sus ventajas y desventajas, y su importancia en la seguridad.

Los Honeypots (Potes de miel) "Consisten en activar un servidor y llenarlo de archivos tentadores, hacer que sea difícil, pero no imposible penetrarlo y sentarse a esperar que aparezcan los intrusos. Los honeynets (conjuntos de honeypots) dan a los crackers un gran espacio para recorrer. Presentan obstáculos que poseen el nivel de complejidad suficiente para atraerlos, pero sin irse al extremo para no desalentarlos... Ellos juegan con los archivos y conversan animadamente entre ellos sobre todo los fascinantes programas que encuentran, mientras el personal de seguridad observa con deleite cada movimiento que hacen. Francamente, siento una combinación de sentimientos con respecto a espiar a la gente, aunque no sean buenas personas". Dan Adams.

También existe el Honeynet, que es un conjunto de Honeypots, así abarca más información para su estudio. Incluso hace más fascinante el ataque al intruso, lo cual incrementa el número de ataques. La función principal a parte de la de estudiar las herramientas de ataque, es la de desviar la atención del atacante de la red real del sistema y la de capturar nuevos virus o gusanos para su posterior estudio. Una de las múltiples aplicaciones que tiene es la de poder formar perfiles de atacantes y ataques.

Son sistemas que deliberadamente se decide exponerlos a ser atacados o comprometidos. Estos, no solucionan ningún problema de seguridad, son una herramienta que nos sirve para conocer las estrategias que se emplean a la hora de vulnerar un sistema. Son una herramienta muy útil a la hora de conocer de forma precisa los ataques que se realizan contra la plataforma de trabajo que hemos elegido, o bien, las plataformas configuradas de la misma forma, y que sirven para guardar todos los procesos que se están ejecutando contra o en nuestro sistema con el claro objetivo de acceder a información sensible para una organización, empresa o corporativo. Así mismo nos permiten conocer nuevas vulnerabilidades y riesgos de los distintos sistemas operativos y diversos entornos y programas, las cuales aún no se encuentren debidamente documentadas.

Durante nuestra investigación hemos podido observar que existen dos tipos de honeypots:

Para la producción y para la investigación. [1]

Honeypots para la investigación:

Gran parte de la atención actual se centra en los honeypots para la investigación, que se utilizan para recolectar información sobre las acciones de los intrusos. El proyecto Honeynet, por ejemplo, es una organización para la investigación sobre seguridad voluntaria, sin ánimo de lucro que utiliza los honeypots para recolectar información sobre las amenazas del ciberespacio.

[1] Tomado del sitio web: http://www.monografias.com/honeypot&honeynet.htm

Honeypots para la producción:

Se les ha prestado menor atención a los honeypots para la producción, que son los que se utilizan para proteger a las organizaciones. Sin embargo, se les concede cada vez más importancia debido a las herramientas de detección que pueden brindar y por la forma cómo pueden complementar la protección en la red y en el host.

1.1.2. Características de los Honeypot

Como características importantes de los honeypots se pueden describir que son de alta o baja interacción, distinción que se basa en el nivel de actividad que le permiten al atacante. Un sistema de baja interacción ofrece actividad limitada; la mayoría de las veces funciona al emular los servicios y sistemas operativos. Las principales ventajas de los honeypots de baja interacción es que son relativamente fáciles de instalar y mantener; también implican un riesgo mínimo porque el atacante nunca tiene acceso a un sistema operativo real para perjudicar a otros sistemas.

"Honeyd" es un ejemplo de honeypot de baja interacción, cuya función principal es monitorear el espacio de direcciones IP no utilizado. Cuando Honeyd detecta un intento de conectarse a un sistema que no existe, intercepta la conexión, interactúa con el atacante fingiendo ser la víctima para captar y registrar al ataque.

Por el contrario, los honeypots de alta interacción utilizan sistemas operativos reales y aplicaciones reales y no emulan nada. Al ofrecerles a los atacantes sistemas reales para que interactúen, las organizaciones

pueden aprender mucho sobre su comportamiento. Los honeypots de alta interacción no imaginan como se comportará un atacante y proporcionan un ambiente que rastrea todas las actividades, lo que les permite a las organizaciones conocer un comportamiento al que de otra manera no tendrían acceso.

Los sistemas de alta interacción también son flexibles y los profesionales de la seguridad de TI pueden implementarlos en la medida que quieran. Además, este tipo de honeypot proporciona un objetivo más realista, capaz de detectar atacantes de mayor calibre. Los honeypots de alta interacción pueden ser complejos de instalar. Sin embargo, requieren que se implementen tecnologías adicionales para evitar que los atacantes los utilicen para lanzar ataques a otros sistemas.

1.1.3. Características de los Honeynet

Los Honeynets son conocidos como Honeypot de alta interacción

Los Honeynets son un ejemplo ideal de honeypots de alta interacción. Honeynets no son un producto, no son una solución software en donde se instala en una computadora. En lugar de eso, los Honeynets son una arquitectura, una entera red de máquinas diseñados para ser atacados. La idea es tener una arquitectura que sea una red altamente controlada, un lugar donde toda actividad sea controlada y capturada. En esta red nosotros ponemos a nuestras victimas en forma intencionada, computadoras reales corriendo aplicaciones reales. Los "chicos malos" encuentran, atacan, rompen estos sistemas en su propia iniciativa. Cuando hacen esto, ellos no saben que están en un Honeynet. Toda su actividad, desde sesiones encriptadas SSH hasta e-mails y archivos subidos son capturados sin que lo noten. Esto es realizado introduciendo módulos en el kernel en los

"sistemas víctima" que capturan todas las acciones de los atacantes. Al mismo tiempo, el Honeynet controla la actividad del atacante. Los Honeynets hacen esto mediante la utilización de un gateway Honeywall. Este gateway permite el tráfico de entrada a los "sistemas víctima", pero controla el tráfico de salida usando tecnologías de prevención contra intrusos. Esto le da al atacante la flexibilidad de interactuar con los sistemas víctimas, pero previene al atacante de dañar otros sistemas que no forman parte del Honeynet.[2]

1.1.4. Sinopsis tecnológica y configuración

Un Honeypot, como el nombre lo indica es un Sistema seductor que haciendo las veces de jarrón de miel atractivo para los hackers, las abejas intrusas, tiene el objetivo de atraerlos para si como si él fuese el sistema real.

Hay que tener muy en cuenta que los Sistemas, funcionan en su afán de presentarse seductoramente, por medio de servidores también cautivadores, que hacen de puente entre el sistema y el intruso.

En las redes se ubican servidores puestos adrede para que los intrusos los saboteen y así son monitorizados por sistemas que actúan como puentes a los servidores, registrando de forma transparente los paquetes que acceden a dichos servidores.

Su funcionamiento está basado en tres simples conceptos:

- Un honeypot no es un sistema de producción y, por tanto, nadie debería tratar de comunicarse con él. No habrá falsos positivos.

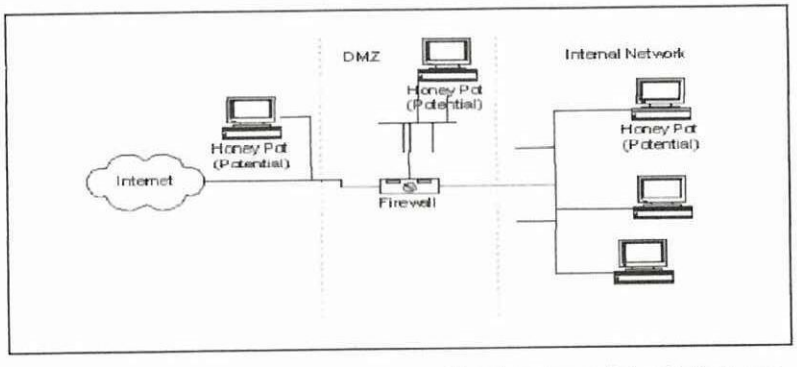
[2] Tomado del sitio web: http://www.adictosaltrabajo.com/honeynet.php

- Cualquier tráfico que tenga por destino el honeypot será sospechoso de ser un sondeo o un ataque.

- Cualquier tráfico que tenga por origen el honeypot significará que el sistema ha sido comprometido.

GRÁFICO 1.1

ESQUEMA DE UN HONEYPOT



Fuente: www.adictosaltrabajo.com

Detectado un ataque (*por modificación de la estructura de archivos*), se recompone la traza del atacante (*secuencia de paquetes registrados en el monitor puente*) y se pasa a un **análisis forense**.

Este análisis forense concluye, en caso de detectar un nuevo ataque, en **una nueva regla de detección**.

Dentro de este criterio de clasificación, el término "Nivel de Interacción" define el rango de posibilidades de ataque que un Honeypot le permite tener un potencial atacante. Estas categorías nos ayudan a entender no solo el tipo de Honeypot con el que se está trabajando, sino también ayudan a definir la gama de opciones en cuanto a las vulnerabilidades que se desea que un atacante explote. Estas son las características de mayor importancia al momento de empezar a construir el perfil de un atacante.

Honeypots de Baja Interacción: Normalmente, estos Honeypots trabajan únicamente emulando servicios y sistemas operativos. La actividad del atacante se encuentra limitada al nivel de emulación del Honeypot. La ventaja de un Honeypot de Baja Interacción radica principalmente en su simplicidad, ya que estos tienden a ser fáciles de utilizar y mantener con un riesgo mínimo. Por ejemplo, un servicio FTP emulado, escuchando en el puerto 21, probablemente estará emulando un login FTP o probablemente suportará algunos comandos FTP adicionales, pero no representa un blanco de importancia crítica ya que probablemente no está ligado a un servidor FTP que contenga información sensible.

Por lo general, el proceso de implementación de un Honeypot de Baja Interacción consiste en instalar un software de emulación de sistema operativo (ej. VMWare Workstation o Server), elegir el sistema operativo y el servicio a emular, establecer una estrategia de monitoreo y dejar que el programa opere por si solo de manera normal. Este proceso, de naturaleza similar al "plug and play", hace que la utilización de este tipo de Honeypot sea extremadamente sencilla. Los servicios emulados mitigan el riesgo de penetración, conteniendo la actividad del intruso que nunca tiene acceso al sistema operativo real donde puede atacar o dañar otros sistemas.

La principal desventaja de los Honeypots de Baja Interacción radica en que registran únicamente información limitada, ya que están diseñados para capturar actividad predeterminada. Debido a que los servicios emulados solo pueden llegar hasta un cierto límite operacional, ésa característica limita la gama de opciones que se pueden anunciar hacia el potencial intruso. De igual manera, es relativamente sencillo para un atacante el detectar un Honeypot de Baja Interacción, ya que un intruso hábil puede detectar qué tan buena es la emulación con el debido tiempo.

Ejemplos de Honeypots de Baja Interacción son: Specter, Honeyd, y KFSensor.

Honeypots de Alta Interacción: Este tipo de Honeypots constituyen una solución compleja, ya que implica la utilización de sistemas operativos y aplicaciones reales montados en hardware real sin la utilización de software de emulación e involucrando aplicaciones reales que se ejecutan de manera normal, muchas veces en directa relación a servicios como bases de datos y directorios de archivos compartidos. Por ejemplo: Si se desea implementar un Honeypot sobre un servidor Linux que ejecute un servidor FTP, se tendrá que construir un verdadero sistema Linux y montar un verdadero servidor FTP.

Las ventajas de dicha solución son dos: Por un lado, se tiene la posibilidad de capturar grandes cantidades de información referentes al *modus operandi* de los atacantes debido a que los intrusos se encuentran interactuando frente a un sistema real. De esta manera, se está en posibilidad de estudiar la extensión completa de sus actividades: cualquier cosa desde nuevos rootkits, zero-days, hasta sesiones internacionales de IRC. Por otro lado, los Honeypots de Alta Interacción no asumen nada acerca del posible comportamiento que tendrá el atacante, proveyendo un entorno abierto que captura todas las actividades realizadas y que ofrece una amplia gama de servicios, aplicaciones y depósitos de información que pueden servir como blanco potencial para aquellos servicios que específicamente deseamos comprometer. Esto permite a las soluciones de alta interacción conocer comportamientos no esperados.

Sin embargo, esta última capacidad también incrementa el riesgo de que los atacantes puedan utilizar estos sistemas operativos reales para lanzar

ataques a sistemas internos que no forman parte de los Honeypots, convirtiendo una carnada en un arma. En consecuencia, se requiere la implementación de una tecnología adicional que prevenga al atacante el dañar otros sistemas que no son Honeypots o que prive al sistema comprometido de sus capacidades de convertirse en una plataforma de lanzamiento de ataques.

Hoy por hoy, el mejor ejemplo de un Honeypot de alta interacción está representado en las Honeynets.

1.1.5. Requisitos del Sistema

Los Honeypots son un concepto increíblemente simple, los cuales ofrecen una fortaleza muy poderosa. Podemos observar sus ventajas en los siguientes puntos:

- Nuevas Herramientas y Tácticas: Son diseñados para capturar cualquier cosa que interactúa con ellos, incluyendo herramientas o tácticas nunca vistas mejor conocidas como 'zero-days'.

- Mínimos Recursos: Esto significa que los recursos pueden ser mínimos y aún así se puede implementar una plataforma lo suficientemente potente para operar a gran escala. Ejemplo: Una computadora con un procesador Pentium con 128 Mb de RAM puede manejar fácilmente una red de clase B entera.

- Encriptación en IPv6: A diferencia de la mayoría de las tecnologías para la seguridad, también trabajan en entornos sobre IPv6. El Honeypot detectará un ataque sobre IPv6 de la misma forma que lo hace con un ataque sobre IPv4.

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

- Simplicidad: Debido a su arquitectura, son conceptualmente simples.

No existe razón por la cual se deba desarrollar o mantener nuevos algoritmos, tablas o firmas. Mientras mas simple sea la tecnología, habrá menos posibilidades de error.

Como cualquier otra tecnología, los Honeypots también tienen debilidades inherentes a su diseño y funcionamiento. Esto se debe a que éstos no reemplazan a las tecnologías actuales, sino que trabajan con las tecnologías existentes:

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

- Riesgo: Inherentemente, el uso de todas las tecnologías de seguridad implican un riesgo potencial. Los Honeypots no son diferentes ya que también corren riesgos, específicamente el de ser secuestrados y controlados por el intruso y ser utilizados como plataforma de lanzamiento de otros ataques.

Aplicaciones Prácticas

Cuando son utilizados con propósitos productivos, los Honeypots proveen protección a la organización mediante prevención, detección y respuesta a un ataque. Cuando son utilizados con propósitos de investigación, éstos recolectan información que depende del contexto bajo el cual hayan sido implementados. Algunas organizaciones estudian la tendencia de las actividades intrusivas, mientras otras están interesadas en la predicción y prevención anticipada.[3]

Los Honeypots pueden ayudar a prevenir ataques en varias formas:

- Defensa contra ataques automatizados: Estos ataques son basados en herramientas que aleatoríamente rastrean redes enteras buscando sistemas vulnerables. Si un sistema vulnerable es encontrado, estas herramientas automatizadas atacaran y tomaran el sistema (con gusanos que se replican en la víctima). Uno de las métodos para proteger de tales ataques es bajando la velocidad de su rastreo para después detenerlos. Llamados "Sticky Honeypots", estas soluciones monitorean el espacio IP no utilizado. Cuando los sistemas son analizados, estos Honeypots interactúan con el y disminuyen la velocidad del ataque. Esto se logra utilizando una variedad de trucos TCP, como poniendo el "Window Size" a cero o poniendo al atacante en un estado de espera continúa. Esto es excelente para disminuir la velocidad o para prevenir la diseminación de gusanos que han penetrado en la red interna.

- Protección contra intrusos humanos: Este concepto se conoce como engaño o disuasión. La idea de esta contramedida es confundir al atacante y hacerle perder tiempo y recursos mientras interactúa con

[3] Tomado del sitio web: www.adictosaltrabajo.com/honeypot.html

el Honeypot. Mientras ese proceso se lleva a cabo, se puede detectar la actividad del atacante y se tiene tiempo para reaccionar y detener el ataque.

- Métodos de Detección Precisa: Tradicionalmente, la detección ha sido una tarea extremadamente difícil de llevar a cabo. Las tecnologías como los Sistemas de Detección de Intrusos y sistemas de logueo han sido deficientes por diversas razones: Generan información en cantidades excesivas, grandes porcentajes de falsos positivos (o falsas alarmas), no cuentan con la habilidad de detectar nuevos ataques y/o de trabajar en forma encriptada o en entornos IPv6. Los Honeypots son excelentes en el ramo de la detección, solventando muchos de los problemas de la detección clásica: Reducen los falsos positivos, capturan pequeñas cantidades de datos de gran importancia como ataques desconocidos y nuevos métodos de explotación de vulnerabilidades (zero-days) y trabajan en forma encriptada o en entornos Ipv6.

- Labor Ciber-Forense: Una vez que un administrador de red se da cuenta que uno o unos de sus servidores fueron comprometidos ilegalmente, es necesario proceder inmediatamente a realizar un análisis forense en el sistema comprometido para realizar un control de daños causados por el atacante. Sin embargo, hay dos problemas que afectan a la respuesta al incidente: Frecuentemente, los sistemas comprometidos no pueden ser desconectados de la red para ser analizados y la cantidad de información que se genera es considerablemente extensa, de manera que es muy difícil determinar lo que hizo el atacante dentro del sistema. Los Honeypots ayudar a solventar ambos problemas, ya que son excelentes herramientas de análisis de incidencias que pueden rápida y fácilmente ser sacados de la red para un análisis forense completo, sin causar impacto en las operaciones empresariales diarias. La única actividad que guardan los Honeypots son las

relacionadas con el atacante, ya que no son utilizadas por ningún otro usuario, excepto los atacantes. La importancia de los Honeypots, es la rápida entrega de la información, analizada en profundidad previamente, para responder rápida y eficientemente a un incidente.

1.1.6. Análisis Informático Forense

En la investigación forense existe una gran debilidad: frente a la evidencia documental, la evidencia digital es frágil, dado que la copia de un documento almacenado en un archivo es idéntica al original. Asimismo, existe el riesgo potencial de realizar copias no autorizadas del archivo original sin que quede evidencia de dicha acción. Por lo anterior, en este tipo de investigaciones se deben cumplir con los principios que citamos a continuación:

Principios para el manejo, recolección y recuperación de evidencia digital.

a) Durante el proceso de recolección de evidencia digital, la evidencia no debe sufrir ningún cambio.

b) Cuando se requiere que una persona tenga acceso a evidencia digital original, dicha persona debe ser un profesional forense.

c) Toda actividad referente a la recolección, el acceso, el almacenamiento o la transferencia de la evidencia digital, debe ser documentada completamente, preservada y disponible para revisión.

d) Mientras la evidencia digital esté en poder de un individuo, éste será totalmente responsable de las acciones tomadas con la misma.

e) Cualquier entidad que sea responsable de recolectar, almacenar o transferir evidencia digital es responsable de cumplir con estos principios.

f) Durante todo el proceso de recolección de evidencia digital, debe haber testigos que certifiquen los procedimientos efectuados.

g) En cuanto al proceso de recuperación, se debe cumplir como mínimo con 4 aspectos fundamentales: capacidad para brindar confianza en cuanto a la integridad de la evidencia, uso de un lenguaje sencillo, aplicabilidad a toda la evidencia forense y ser consistente con todos los sistemas legales.

En lo referente a las **herramientas para la investigación forense;** existe una gran variedad y dependen del objetivo para la cual van a ser utilizadas. Existen para la recolección de evidencia (las de mayor importancia en la computación forense), para el monitoreo o control de computadores, para el marcado de documentos y de hardware (dispositivos físicos para la recolección de evidencia).

Ahora, toda investigación forense en términos generales involucra como mínimo para su desarrollo **cuatro pasos** que enunciamos a continuación y explicamos con mayor detalle en secciones posteriores:

a) Preparación y conocimiento general.

b) Recolección y manipulación.

c) Inspección y análisis de la evidencia.

d) Reconstrucción de los hechos.

Finalmente, en cuanto las **dificultades** que podría tener el investigador forense, se relacionan con factores como su habilidad, experiencia, carencia de herramientas especializadas, deficientes o inexistentes rastros de auditoria o resistencia por parte de algunos funcionarios de la entidad para la entrega o dar acceso a la información de la entidad (en la exposición del caso, se presenta de manera práctica esta problemática) [4]

1.2. SISTEMAS DE DETECCION DE INTRUSOS

1.2.1. Definiciones de Intrusos e Intrusiones

Para poder planear e implementar una buena estrategia de seguridad, primero debe tener en cuenta algunos de los problemas que un atacante motivado y determinado explota para comprometer sus sistemas. Pero antes de detallar estos problemas, debemos definir la terminología usada para identificar un atacante.

El significado moderno del término *hacker* tiene sus orígenes en los años 60 y en el Club de Modelaje de Trenes del Instituto de Tecnología de Massachusetts (MIT), que diseñaban conjuntos de trenes de gran escala y detalle. Hacker fue el nombre usado para nombrar aquellos miembros del club que descubrían un truco brillante o que resolvían un problema muy complicado.

[4] Tomado del libro: Redes de Computadoras TANENBAUM, Andrew S. Editorial Prentice Hall Quinta Edición. Año 2007, Pagina 754 - 756.

Desde ese momento el término hacker se ha utilizado para describir cualquier cosa desde un aficionado a las computadoras hasta un programador virtuoso. Un rasgo característico de un hacker es su disposición de explorar en detalle cómo funcionan los sistemas de computación con poca o ninguna motivación externa. Los desarrolladores de software de la comunidad de Código Abierto (Open Source), a menudo se consideran a ellos mismos y a sus colegas como hackers, como una forma de respeto.

Típicamente, los hackers siguen una forma de *ética de hackers* que dicta que la búsqueda de información y experiencia es esencial y que compartir ese conocimiento es el compromiso de todo hacker con la comunidad. Durante esa búsqueda de conocimiento, algunos hackers disfrutan los retos académicos de burlar los controles de seguridad en sistemas de computación. Por esta razón, la prensa usualmente utiliza este término para describir aquellos que accesan sistemas y redes ilegalmente sin escrúpulos, con intenciones maliciosas o criminales. El término más adecuado para este tipo de hacker de computadoras es *cracker* o *maleante informático* (también se les conoce como *pirata informático*, *ciberpirata*, etc.). Un término creado por los hackers en la mitad de los 80 para diferenciar a las dos comunidades.[5]

1.2.2. Tipos de Intrusos e Intrusiones

Dentro de la comunidad de individuos que intentan encontrar y explotar las vulnerabilidades en sistemas y redes, se encuentran varios grupos distintos. Estos grupos se describen por el color del sombrero que ellos

[5] Tomado del libro: Redes de Computadoras TANENBAUM, Andrew S. Editorial Prentice Hall Quinta Edición. Año 2007, Pagina 674 – 675, 701.

usan cuando realizan sus investigaciones de seguridad, y este tono es un indicativo de su intención.

Un *hacker de sombrero blanco* es aquel que prueba sistemas y redes para examinar su rendimiento y determinar que tan vulnerables estos son ante un intruso. Usualmente, los hackers de sombrero blanco tratan de violar sus propios sistemas o los sistemas de un cliente el cual lo ha empleado particularmente para propósitos de auditoria de seguridad.

Los investigadores de seguridad y los consultores de seguridad profesional son dos ejemplos de hackers de sombrero blanco.

Un *hacker de sombrero negro* es sinónimo de un cracker. En general, los crackers están menos enfocados en el lado de programación y académico de violar un sistema. Con frecuencia los crackers utilizan programas especializados para violar vulnerabilidades conocidas en los sistemas para así descubrir información confidencial para beneficio personal o para producir daños a un sistema o red.

Por otro lado, un *hacker de sombrero gris*, tiene las habilidades e intenciones de un hacker de sombrero blanco pero en la mayoría de las situaciones utiliza ese conocimiento para propósitos menos nobles.

Un hacker de sombrero gris se puede ver como un hacker de sombrero blanco el cual a veces usa un sombrero negro para ejecutar su propia agenda.

Los hackers de sombrero gris usualmente se suscriben a otra forma de código de ética que dice que es aceptable entrar en un sistema siempre y cuando el hacker no cometa robo o viole la confidencialidad.

Sin embargo, otros argumentan que el sólo hecho de violar un sistema es por sí mismo antiético.

No importa cual sea la intención, es importante conocer las debilidades que un pirata intentará explotar.

1.2.3. Sistemas Operativos soportados

1.2.3.1. Linux

Linux es probablemente el acontecimiento más importante del software gratuito desde el original Space War, o, más recientemente, Emacs. Se ha convertido en el sistema operativo para los negocios, educación, y provecho personal. Linux ya no es solo para gurus de UNIX que se sientan durante horas frente a la resplandeciente consola (aunque le aseguramos que un gran número de usuarios pertenece a esta categoría). Este libro le ayudara a sacarle el máximo partido.

Linux (pronunciado con una i corta, como en LIH-nucs) es un clonico del sistema operativo UNIX que corre en ordenadores Intel 80386 y 80486. Soporta un amplio rango de software, desde TEX a X Windows al compilador GNU C/C++ a TCP/IP. Es una implementación de UNIX versátil, distribuida gratuitamente en los términos de la Licencia GNU.

Linux puede convertir cualquier PC 386 o 486 en una estación de trabajo. Le pondrá todo el poder de UNIX en la punta de sus dedos. En los negocios ya se instala Linux en redes enteras, usando el sistema operativo para manejar registros financieros y de hospitales, un entorno de usuario distribuido, telecomunicaciones, etc. Universidades de todo el mundo usan Linux para dar cursos de programación y diseño de sistemas operativos. Y, por supuesto, entusiastas de los ordenadores de todo el mundo están usando Linux en casa, para programar, entretenerse, y conocerlo a fondo.

Lo que hace a Linux tan diferente es que es una implementación gratuita de UNIX. Fue y aun es desarrollado por un grupo de voluntarios, principalmente en Internet, intercambiando código, comentando fallos, y arreglando los problemas en un entorno abierto. Cualquiera es bienvenido a sumarse al esfuerzo de desarrollo de Linux: todo lo que se pide es interés en producir un clónico gratuito de UNIX y algunos conocimientos de programación.

1.2.3.2 Windows 2003

Microsoft Windows (conocido simplemente como *Windows*) es un sistema operativo con interfaz gráfica para computadoras personales cuyo propietario es la empresa Microsoft. Las distintas versiones de Windows, las cuales ofrecen un entorno gráfico sencillo desde la versión Windows 95. Se ha convertido en el sistema operativo más utilizado en el mundo. Por ésta razón, la mayoría de las empresas fabricantes de hardware y software en el mundo tienden a desarrollar sus aplicaciones basadas en dicho sistema. El común uso de éste sistema operativo se debe a que la mayoría de las computadoras incluyen éste sistema instalado por defecto. Esto causa cierta controversia, ya que es visto por ciertas personas, como

un método monopolista de Microsoft, ya que obliga al cliente a comprar una licencia de Microsoft, al mismo tiempo que compra la máquina.

Windows ha incorporado a través de sus diferentes versiones varias herramientas que se han convertido en estándares internacionales, como por ejemplo, el sistema de archivos FAT. Windows incorpora, entre otro software, herramientas como Internet Explorer y el Reproductor de Windows Media. Estas herramientas se han convertido con el tiempo en las más usadas, especialmente Internet Explorer, debido a que vienen instaladas por defecto en dicho sistema operativo.

Windows es utilizado principalmente en computadoras personales existiendo también diferentes versiones para servidores y dispositivos móviles.[6]

1.2.3.3 Solaris

Solaris es un sistema operativo desarrollado por Sun Microsystems. Es un sistema certificado como una versión de UNIX. Aunque Solaris en sí mismo aún es software propietario, la parte principal del sistema operativo se ha liberado como un proyecto de software libre denominado *Opensolaris*. Solaris puede considerarse uno de los sistemas operativos más avanzados. Sun denomina así a su sistema operativo.

[6] Tomado de los sitios web: www.linuxparatodos.com/index.html, www.linux.mx/historiadelkernel.php, www.linux.es/definiciones.jhtml, www.proyectolinux.ar.

El primer sistema operativo de Sun nació en 1983 y se llamó inicialmente **SunOS**. Estaba basado en el sistema UNIX BSD, de la Universidad de Berkeley, del cual uno de los fundadores de la compañía fue programador en sus tiempos universitarios. Más adelante incorporó funcionalidades del System V, convirtiéndose prácticamente en un sistema operativo totalmente basado en System V.

Esta versión basada en System V fue publicada en 1992 y fue la primera en llamarse **Solaris**, más concretamente *Solaris 2*. Las anteriores fueron llamadas *Solaris 1* con efecto retroactivo. SunOS solo tendría sentido a partir de ese momento como núcleo de este nuevo entorno operativo Solaris. De esta forma Solaris 2 contenía SunOS 5.0. Desde ese momento se distingue entre el núcleo del sistema operativo (SunOS), y el entorno operativo en general (Solaris), añadiéndole otros paquetes como Apache o DTrace. Como ejemplo de esta función, Solaris 8 contiene SunOS 5.8.

Solaris usa una base de código común para las arquitecturas que soporta: SPARC y x86 (incluyendo AMD64/EM64T). También fue portado a la arquitectura PowerPC (en plataforma PReP) en la versión 2.5.1, pero el porte fue cancelado casi tan pronto como fue liberado. En un tiempo se planeó soporte para el Itanium pero nunca se llevó al mercado. [1] Sun también tiene planes de implementar ABIs de Linux en Solaris 10, permitiendo la ejecución de código objeto Linux de forma nativa en la plataforma x86.

Solaris tiene una reputación de ser muy adecuado para el multiprocesamiento simétrico (SMP), soportando un gran número de CPUs. También ha incluido soporte para aplicaciones de 64 bits SPARC

desde Solaris 7. Históricamente Solaris ha estado firmemente integrado con la plataforma hardware de Sun, SPARC, con la cual fue diseñado y promocionado como un paquete combinado. Esto proporcionaba frecuentemente unos sistemas más fiables pero con un coste más elevado que el del hardware de PC. De todas formas, también ha soportado sistemas x86 desde la versión Solaris 2.1 y la última versión, Solaris 10, ha sido diseñada con AMD64 en mente, permitiendo a Sun capitalizar en la disponibilidad de CPUs de 64 bits commodities basadas en la arquitectura AMD64. Sun ha promocionado intensamente Solaris con sus estaciones de trabajo de nivel de entrada basadas en AMD64, así como con servidores que en 2006 varían desde modelos dual-core hasta modelos a 16 cores.

El primer entorno de escritorio para Solaris fue OpenWindows. Fue reemplazado por CDE en la versión Solaris 2.5. El escritorio Java Desktop System, basado en GNOME, se incluye por defecto con Solaris 10.

El código fuente de Solaris (con unas pocas excepciones) [2] ha sido liberado bajo la licencia CDDL (**Licencia Común de Desarrollo y Distribución**) como un proyecto de software libre bajo el nombre **OpenSolaris**.

La licencia CDDL ha sido aprobada por la Open Source Initiative (OSI) como una licencia open source y por la FSF como una licencia de software libre (aunque incompatible con la popular licencia GPL).

La base de OpenSolaris fue alimentada el 14 de junio de 2005 a partir de la entonces actual base de desarrollo de código de Solaris. Es posible

descargar y licenciar versiones tanto binarias como en forma de código fuente sin coste alguno. Además, se ha añadido al proyecto Open Solaris código para características venideras como soporte Xen. Sun ha anunciado que las versiones futuras de Solaris se derivarán a partir de OpenSolaris.[7]

1.3. SISTEMA DE SEGURIDADES

1.3.1. Definición de Seguridad

Debido a la creciente confianza en computadoras de red poderosas para los negocios y en llevar un seguimiento de nuestra información personal, las industrias se forman considerando de antemano la práctica de seguridad de la computación y redes. Las corporaciones solicitan el conocimiento y habilidades de los expertos para auditar los sistemas y ajustar soluciones para satisfacer los requerimientos operativos de la organización. Puesto que la mayoría de las organizaciones son dinámicas por naturaleza, con trabajadores accesando los recursos informáticos de la organización local y remotamente, la necesidad de ambientes computacionales seguros se ha vuelto cada vez más relevante.

Desafortunadamente, la mayoría de las organizaciones (así como también usuarios individuales) dejan la seguridad como algo para resolver luego, un proceso que es ignorado en favor de mayor poder, mayor productividad y en las preocupaciones presupuestarias. La implementación adecuada de la seguridad es a menudo realizada *postmortem*. Después que ocurre una intrusión no autorizada. Los expertos de seguridad consideran que el establecimiento de medidas adecuadas antes de conectar un sitio a una red insegura tal como la Internet, es una forma efectiva de frustrar la mayoría de los intentos de intrusión.

[7] Tomado del sitio web: www.palosanto.com, sitio de soporte para este tipo de sistemas operativos

La seguridad de computación es un término general que cubre una gran área de computación y procesamiento de la información. Las industrias que dependen de sistemas computarizados y redes para ejecutar sus operaciones y transacciones de negocios diarias, consideran sus datos como una parte importante de sus activos generales. Muchos términos y medidas se han incorporado a nuestro vocabulario diario en los negocios, tales como costo total de propiedad (total cost of ownership, TCO) y calidad de servicios (QoS). Con estas medidas, las industrias calculan aspectos tales como integridad de los datos y alta disponibilidad como parte de los costos de planificación y administración de procesos.

En algunas industrias, como el comercio electrónico, la disponibilidad y confianza de los datos pueden hacer la diferencia entre el éxito y el fracaso.

Muchos de nosotros que gustamos del cine tuvimos la oportunidad de mirar la película "Juegos de guerra," protagonizada por Matthew Broderick haciendo el papel de un estudiante de educación secundaria que logra entrar en el supercomputador del Departamento de Defensa (DoD) de los Estados Unidos y, sin darse cuenta, causa una amenaza de guerra nuclear. En esta película, Broderick utiliza un módem para conectarse con el computador del DoD (llamado WOPR) y juega juegos con el software de inteligencia artificial que controla los silos de misiles nucleares. La película fue estrenada durante la "guerra fría" entre la antigua Unión Soviética y los Estados Unidos y fue considerada un éxito en 1983. La popularidad de la película inspiró a muchas personas y grupos a comenzar la implementación de algunos métodos que el joven protagonista utilizó para violar los sistemas restringidos, incluyendo lo que se conoce como *war dialing* o *ataque de marcado.* Un método de búsqueda de números telefónicos para conexiones de módem analógico en un código de área definido y con una combinación prefija del número.

Más de 10 años después, después de cuatro años de búsquedas en diferentes jurisdicciones implicando al Federal Bureau of Investigation (FBI) y con la ayuda de varios profesionales de computación a lo largo del país, fue arrestado el infame maleante informático (cracker) Kevin Mitnick y culpado con más de 25 cargos por fraude de computadores y dispositivos. Estos fraudes resultaron en un estimado de US$80 Millones en pérdidas de propiedad intelectual y código fuente de Nokia, NEC, Sun Microsystems, Novell, Fujitsu y Motorola. Para esa fecha, el FBI lo consideró la ofensa criminal de computación más grande en la historia de los EEUU. Mitnick fue apresado y sentenciado a 68 meses en prisión por sus crímenes, de los cuales sirvió un total de 60 antes de obtener libertad condicional

El 21 de Enero del 2000. A Mitnick se le ha prohibido utilizar computadoras o hacer ningún tipo de consultoría relacionada con computadoras hasta el año 2003. Los investigadores dicen que Mitnick era un experto en *ingeniería social* .usando personas para ganar acceso a las contraseñas y sistemas usando credenciales falsificadas.

La seguridad de la información ha evolucionado en los últimos años debido al incremento de la confianza en las redes públicas para manejar información personal, financiera y otra información restringida.

La popularidad de la Internet ha sido uno de los factores más importantes que ha incitado e intensificado los esfuerzos para la seguridad de los datos. Cada día hay más personas que utilizan sus computadores personales para ganar acceso a los recursos que la Internet tiene que ofrecer. Desde investigaciones o recuperación de la información hasta correo electrónico y transacciones comerciales, la Internet ha sido reconocida como uno de

los desarrollos más importantes del siglo 20. La Internet y sus primeros protocolos, sin embargo, fueron desarrollados como un *sistema basado en confianza*. Esto es, el Protocolo de Internet no fue diseñado para ser seguro en sí mismo. No existen estándares de seguridad aprobados incorporados en las comunicaciones TCP/IP, dejándolas abiertas a potenciales usuarios maliciosos y procesos en la red. Los desarrollos modernos han hecho de las comunicaciones en Internet más seguras, pero todavía hay muchos incidentes que capturan la atención a nivel nacional y nos alertan del hecho de que nada es completamente seguro.

1.3.2. Tipos de Seguridades en Redes de Telecomunicaciones a nivel de Servidores

Cuando un sistema es usado como un servidor en una red pública, se convierte en un objetivo para ataques. Por esta razón, es de suma importancia para el administrador fortalecer el sistema y bloquear servicios.

Antes de extendernos en problemas particulares, debería revisar los siguientes consejos generales para mejorar la seguridad del servidor:

- Mantenga todos los servicios actualizados para así protegerse de las últimas amenazas informáticas.
- Utilice protocolos seguros siempre que sea posible.
- Proporcione sólo un tipo de servicio de red por máquina siempre que sea posible.
- Supervise todos los servidores cuidadosamente por actividad sospechosa.

Con el tiempo suficiente, los recursos y la motivación, un intruso puede violar casi cualquier sistema. Al final del día, todos los procedimientos de seguridad y la tecnología disponible actualmente no pueden garantizar que sus sistemas estén seguros de un ataque. Los enrutadores lo pueden ayudar a asegurar sus puertas de enlace (gateways) a la Internet. Los cortafuegos (firewalls) le permiten asegurar el borde de su red. Las redes privadas virtuales pueden pasar con seguridad sus datos en un flujo encriptado. Los sistemas de detección de intrusos pueden advertirlo de actividades maliciosas.

Sin embargo, el éxito de cada una de estas tecnologías depende de un número de variables, incluyendo:

- La experiencia del personal responsable de la configuración, supervisión y mantenimiento de las tecnologías.
- La habilidad de remendar y actualizar servicios y kernels rápida y eficientemente.
- La habilidad de aquellos responsables de mantener vigilancia constante sobre la red.

Dado el estado dinámico de los sistemas de datos y tecnologías, asegurar sus recursos corporativos puede ser bien complejo. Debido a esta complejidad, puede ser difícil encontrar recursos expertos para todos sus sistemas. Mientras que es posible tener personal con conocimientos en muchas áreas de seguridad de información a un nivel alto, es difícil mantener personal que sea experto en más de unas pocas áreas particulares. Esto se debe principalmente a que cada área en particular de

seguridad de la información requiere constante atención y foco. La seguridad de información no se queda quieta. [8]

[8] Tomado del libro: REDES GLOBALES DE INFORMACION CON INTERNET Y TCP/IP de COMER Douglas E. Editorial prentice Hall, Tercera edición año 2006

CAPITULO II

2. TRABAJO DE CAMPO

ELEMENTOS NECESARIOS PARA LAS CONFIGURACIONES DE LOS SERVIDORES TRAMPA (HONEYPOT)

2.1. Parámetros necesarios a ser considerados en las configuraciones de los Honeypot

Un *honeypot* puede ser tan simple como un ordenador que ejecuta un programa escuchando en cualquier número de puertos. Al programa, al sistema operativo, al protocolo o a cualquier otro elemento de la cadena se le mantiene una vulnerabilidad o debilidad que lo haga más goloso y cree confianza en el pirata, de manera que se muestre dispuesto a emplear todas sus habilidades para explotarlo y ganar acceso al sistema.

Por otro lado, un *honeypot* puede ser tan complejo como una completa red de ordenadores completamente funcionales corriendo bajo distintos sistemas operativos y ofreciendo gran cantidad de servicios, y hacer que cuando alguna computadora que lo comprende sea escaneada, se advierta al administrador mediante e-mail, SMS o cualquier otro sistema de alerta.
Pero también puede ser todo virtual, los hay ya listos para ser usados, programas específicamente diseñados para simular una red, engañar al pirata con direcciones falsas, IP fingidas y ordenadores inexistentes, con el único fin de confundir al hacker creyendo que ha entrado y tiene acceso a una red inmensa donde, con toda probabilidad, habrá un montón de miel

lista para ser probada. Pero se equivoca, si algo tienen en común los *honeypots* es que no guardan ninguna información relevante, y si lo parece, (si se muestran contraseñas o datos de usuario) son completamente ficticios.

Por último, se puede construir uno mismo un *honeypot* artesano, hecho a mano, abriendo pequeñas brechas de seguridad a conciencia y teniendo en cuenta hasta el último detalle. Esto se hace, en general, para comprobar qué clase de motivaciones atraen más a los atacantes, no sólo humanos, también se puede estudiar el comportamiento de un gusano o virus que se conoce ataca una vulnerabilidad concreta.

Preparar un ordenador tarado con esa vulnerabilidad y diseñar en sus "bambalinas" todo un sistema de alerta y rastreo que registre paso a paso la actividad del gusano puede ser gran utilidad a la hora de programar una vacuna y, en definitiva, "conocer al enemigo".

Como toda herramienta destinada mejorar la seguridad, los *honeypots* tienen sus ventajas e inconvenientes. Su mayor utilidad radica en su simpleza. Al ser un mecanismo cuyo único fin consiste en que intenten abusar de él, no realiza ningún servicio real, y el tráfico que transita a través de él va a ser muy pequeño.

Si se detecta tráfico que va o viene hacia el sistema, casi con toda probabilidad va a ser una prueba, escaneo o ataque. El tráfico registrado en un sistema de este tipo es sospechoso por naturaleza, por lo que su gestión y estudio se simplifica en gran medida. Aunque, por supuesto, ocurran "falsos positivos", expresión que, en este caso, invierte su significado. Si

un falso positivo se produce normalmente cuando una actividad sospechosa tomada como ataque no resulta serlo, en el ambiente de los "tarros de miel", el falso positivo sería el tráfico gestionado por la máquina que no representa una amenaza. En esta simpleza de uso de tráfico y recursos, radica su mayor ventaja. En resumen, poca información, pero muy valiosa.

Entre los problemas que puede causar, destaca la posibilidad de que se vuelva en nuestra contra. Si no se diseña de una manera absolutamente estudiada, si no se ata cada cabo, el pirata puede acabar llevándose el cebo sin ser atrapado por la caña. Si descubre alguna otra vulnerabilidad no prevista o consigue burlar los sistemas de registro, puede usar el ordenador atacado como plataforma para otros ataques o, lo que representaría un completo fracaso del sistema, comprometer máquinas reales con datos valiosos conectados al *honeypot*.

Los hackers no son estúpidos, saben que existen herramientas destinadas para darles caza, y antes de dejarse llevar ante una víctima, realizan varias comprobaciones "rutinarias" que les ayudan a conocer a qué tipo de sistemas se están enfrentando. Esto puede ser un problema para los tarros de miel. Por ejemplo, un *honeypot* puede estar diseñado para emular un servidor web IIS bajo Windows 2000, pero correr bajo un servidor Unix Solaris. Hay gran variedad de métodos para que el propio servidor nos comunique algunas pistas de lo que es y qué contiene. Si se llega a averiguar esta contradicción, el pirata sospechará enseguida y abandonará el sistema sin realizar más ataques.

Honeynet es el nombre que se le ha dado al tipo de *honeypot* específicamente diseñado para la investigación. Si los *honeypot*s pueden

ser usados por una empresa privada para detectar ataques de manera más fácil, rápida y efectiva, en vez de tener que desenvolverse entre gigas y gigas de logs almacenados, las honeynet tienen el propósito principal de investigar el uso de las técnicas y herramientas que hacen los chicos malos de Internet.

Se diferencia básicamente en que no supone una sola máquina, sino múltiples sistemas y aplicaciones que emulan otras tantas, imitan vulnerabilidades o servicios conocidos o crean entornos "jaula" donde mejor observar los ataques. Los requerimientos básicos e imprescindibles para construir una *honeynet* son: Data Control (control de datos) y Data Capture (captura de datos).

Los Data Control suponen la contención controlada de la información y las conexiones. Lidiar con hackers siempre supone un riesgo que hay que reducir al máximo, por lo que es preciso asegurarse que una vez comprometido el *honeypot*, no se comprometerán sistemas legítimos. El reto consiste en mantener un absoluto control del flujo de datos sin que el pirata lo note. No se puede cerrar un sistema por completo para evitar el tráfico innecesario. Una vez comprometido el sistema, el hacker intentará realizar distintos tipos de conexiones para continuar su ataque, probablemente necesite bajar programas por ftp, correo o conexiones SSH. Si no se le permite esta flexibilidad de acciones, además de levantar sus sospechas, no se podrán estudiar uno de los pasos más importantes que valdría la pena analizar. En los primeros intentos de los investigadores de poner en marcha proyectos de *honeynet*, no se permitieron ningún tipo de conexiones salientes para evitar ser plataforma de nuevos ataques. Pero sólo les llevaba a los atacantes unos diez minutos ver que algo andaba mal, y abandonar el intento de ataque. Los resultados así eran muy pobres. De

esto se deduce una disyuntiva en la que reside el arte de una buena red de miel.

Es necesario encontrar el equilibrio entre la libertad de movimientos para el hacker, que supone un mayor riesgo, y la seguridad real del sistema, que puede derivar en resultados menos interesantes para el estudio.

El otro punto fuerte de las *honeynets* es el Data Capture, o el rastreo y almacenamiento de la información que perseguimos, o sea, los logs de sus actos que serán analizados a posteriori. Se debe capturar tanta información como sea posible aislada del tráfico legal, evitando la posibilidad de que el hacker sepa que se le está "grabando en vivo". Lo más importante para conseguir esto, es no guardar los resultados localmente en el *honeypot*, pues pueden ser potencialmente detectados y borrados con la lógica intención de no dejar huellas del ataque. La información debe ser almacenada remotamente y en capas. No se puede limitar al registro de una simple capa de información, sino tomarla de la mayor variedad posible de recursos. Combinándolos, las capas formarán el cuadro deseado.

2.2. Estándares de calidad de servicio y rendimiento a seguir para la instalación y configuraciones de los Servidores Honeypot

Las propiedades de gran valor necesitan ser protegidas de robo o destrucción potencial. Algunos hogares están equipados con sistemas de alarmas que pueden detectar ladrones, notificar a las autoridades cuando ocurre una entrada ilegal y hasta advertir a los dueños cuando sus hogares están bajo fuego.

Tales medidas son necesarias para asegurar la integridad de los hogares y la seguridad de sus dueños. El mismo aseguramiento de la integridad y seguridad debería ser aplicado a los sistemas de computación y datos. La Internet ha facilitado el flujo de la información, desde personal hasta financiera.

Al mismo tiempo, también ha promovido muchos peligros. Los usuarios maliciosos y crackers buscan objetivos vulnerables tales como sistemas no actualizados, sistemas infectados con troyanos y redes ejecutando servicios inseguros. Las alarmas son necesarias para notificar a los administradores y a los miembros del equipo de seguridad que ha ocurrido una entrada ilegal para que así estos puedan responder en tiempo real a la amenaza. Se han diseñado los *sistemas de detección de intrusos* como tales sistemas de notificación.

Aún cuando tcpdump es considerada una herramienta de auditoria muy útil, no se considera un verdadero Honeypot puesto que no analiza ni señala paquetes por anomalías. tcpdump imprime *toda* la información de paquetes a la salida en pantalla o a un archivo de registro sin ningún tipo de análisis. Un verdadero IDS analiza los paquetes, marca las transmisiones que sean potencialmente maliciosas y las almacena en un registro formateado.

Snort es un Honeypot diseñado para ser completo y preciso en el registro de actividades maliciosas de la red y en notificar a los administradores cuando existe una potencial violación o abertura. Snort utiliza la librería estándar libcap y tcpdump como registro de paquetes en el fondo.

La característica más apreciada de Snort, además de su funcionalidad, es su subsistema flexible de armas de ataques. Snort tiene una base de datos de ataques que se está actualizando constantemente y a la cual se puede añadir o actualizar a través de la Internet. Los usuarios pueden crear 'Armas' basadas en las características de los nuevos ataques de red y enviarlas a la lista de correo de armas de Snort (localizada en http://www.snort.org/lists.html), para que así todos los usuarios de Snort se puedan beneficiar. Esta ética de comunidad y compartir ha convertido a Snort en uno de los IDSes basados en red más populares, actualizados y robustos.

2.3.Logros e Insuficiencias encontradas en la manera de implementación en equipos físicos

La implementación de equipos trampa siempre va a traer consigo muchas dudas ya que las empresas y las instituciones consideran que es un desperdicio de algún equipo físico (Servidor) o que va a mermar el rendimiento de algún servidor o de la misma red, más lo que se pretende es demostrar que un servidor de este tipo ayudaría a los administradores del departamento de sistemas a saber con se cuenta de que se debe cuidar y de quien.

Es importante hacer notar que la diferencia entre un departamento de sistemas que cuenta con un servidor trampa y otro que no lo tiene es que en el uno se conoce de que se cuida y en el otro no se conoce si se tiene que cuidar de algo o de alguien.

En el Internet existían según las estadísticas 47 millones de páginas web hasta el año 2003 pero hasta el año 2006 las paginas web habrían aumentado a 76 millones de paginas, en el ultimo año es decir hasta el 2007 las paginas web

sobre pasaron las 100 millones, y por lo tanto la investigación y las ganas de saquear la información aumenta.

Sin embargo según el mismo sitio web: www.growth.com en los Estados Unidos de América el 75% de empresas o personas que navegan en el Internet tienen la etnología de Firewall para poder precautelar la información personal o corporativa, el restante porcentaje se cuida con IDS o con Certificados Digitales y en un reducido número que no alcanza el 5% se protege con un antivirus. Lo que podemos concluir es que en nuestro país estamos tecnológicamente en pañales ya que las cifras son infinitamente inferiores ya que ni siquiera se cuenta con un informe exacto de cuantas empresas utilizan una u otra Tecnología para poder proteger su información.

Nuestra investigación fue mucho mas adelante y trato de muchos ataques que se los realizan a páginas web tanto a nivel mundial como a nivel local de parte de hackers que tratan de buscar un poco de publicidad o sobresalir en el Internet.

Según el sitio WEB: www.gocsi.com y www.securitystats.com, en el Departamento de Defensa de los Estados Unidos de América (DoD., USA), de 8932 ataques Informáticos que se los realiza 7860 fueron realizados con algún éxito, o que se los pudo catalogar como exitosos porque lograron entrar en las seguridades u obtuvieron algún tipo de información y apenas 360 ataques fueron detectados.

Las estadísticas en cambio manifiestan que desde el año de 1998 hasta la actualidad han existido más de 325 ataques exitosos a páginas web ecuatorianas según lo manifiestan paginas web como la: www.zone-h.org, los sitios que fueron hacheados están por ejemplo:

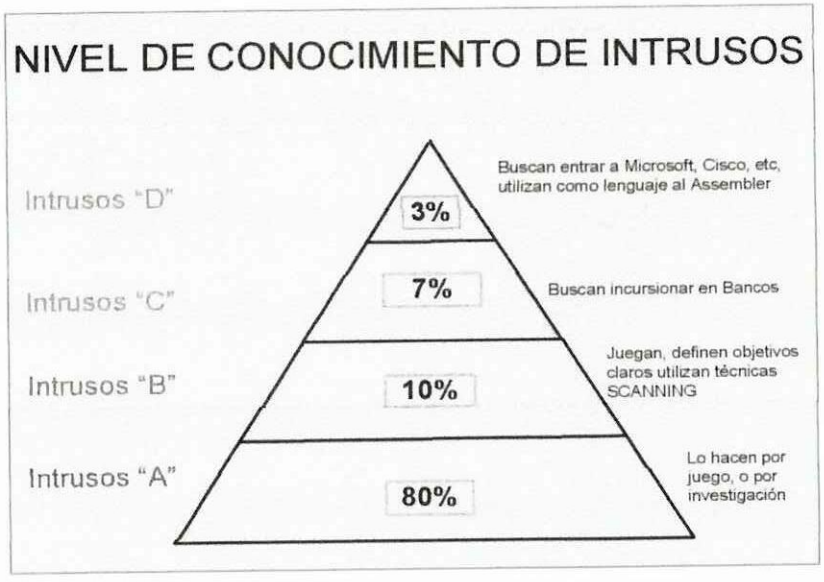
www.sigob.gov.ec (13/02/2004)

www.tvcable.com.ec (04/08/2003)

Dentro de esta cronología hemos podido detectar la existencia de 4 tipos de intrusos los mismos que atacan las páginas web o las instalaciones informáticas de una empresa con distintos lenguajes de programación, o de distintas maneras.

FIGURA 2.1

NIVEL DE CONOCIMIENTO DE INTRUSOS



Fuente: Grupo Investigador

En el grafico anterior se puede observar claramente como se los puede identificar a los distintos hackers los mismos que realizan sus actividades buscando satisfacer sus egos profesionales y tecnológicos.

También podemos notar que en un alto porcentaje lo que tratan es de investigar o lo hacen por simple curiosidad, y en algunas ocasiones causando daños irreversibles que afectan económicamente a la mayoría de

empresas que tienen información en la web, o que básicamente cuentan con una pagina web dinámica.

El porcentaje más bajo son de aquellos usuarios que tienen un nivel académico alto y que tratan de atentar en contra de empresas grandes tecnológicamente como es el caso de Microsoft, Cisco, o el mismo Departamento de Defensa de los Estados Unidos que invierten grandes cantidades de dinero en seguridad de la información.

2.4.Análisis de los resultados obtenidos de las fuentes consultadas, a nivel de administración de departamento de Sistemas Área de Seguridad, docentes y estudiantes de la especialidad de Sistemas

Para la elaboración del presente trabajo investigativo se pudo recabar información de empresas e instituciones en donde laboran personas amigas como son el caso de los Ing. Fabricio Tamayo Gerente General de la Empresa Biologic Sofá de la ciudad de Quito, el Ing. Diego Guanoluisa empleado del Ilustre Municipio de la ciudad de Latacunga, los Ing. Juan Rodríguez, Ing. Patricio Navas, Ing. Matius Mendoza, todos estos docentes de la carrea de Ciencias de la Ingeniería y Aplicadas, así como también se pudo recoger el criterio del administrador de las redes de la Universidad como es el caso del Ing. Miguel Cerda.:

Nuestras preguntas realizadas a los profesionales fueron muy diversas siempre tratando de recabar la mayor cantidad de información posible que pueda ser un aporte para nuestro trabajo de investigación.
Las preguntas fueron muy variadas y en muchas ocasiones intercambiamos criterios sobre como se deberían tener las seguridades las empresas o instituciones.

La pregunta más trascendental en nuestra investigación fue cuanto conocían sobre los HONEYPOT, obtuvimos variadas respuestas ya que al tratarse de éste que es nuevo en nuestro país poco se conocía y más bien nos manifestaban alternativas a este tipo de seguridad, tal como los IDS, los IPS que son maneras de prevenir y más no de detectar y contrarrestar.

Sobre el funcionamiento de los Honeypot se nos manifestó que actúan tanto de forma externa como de forma interna en servidores y en las redes y que regularmente son encontrados o detectados por:

- Scanner de Vulnerabilidades
- Scanner de Puertos
- Exploits (Son formas de explotar las vulnerabilidades).

Es necesario indicar que la información de honeypot es muy común encontrar hoy en día en el Internet y paginas que se dedican a la difusión de maneras de prevenir la información de usuarios maliciosos de la red.

Les preguntamos si las implementarían en sus empresas como medio para prevenir posibles ataques de hackers y nos manifestaban casi en su totalidad coinciden en que todavía es una herramienta muy nueva y que las empresas hasta no tener bien probadas las mismas no invierten en este tipo de tecnología, a lo que les manifestamos que siempre es bueno prevenir y más ahora que existen muchas alternativas para evitar los ataques de los hackers que buscan infiltrarse en las empresas solamente con el objetivo de causar daños a la información aunque no reciban rédito alguno.

Un honeypot utiliza recursos de un servidor ya que actúa como tal, pero se lo podría simular mediante la utilización de Virtual Machines que de tiempo a está parte se ha convertido en una herramienta indispensable al momento de implementar servidores sean estos Open Source o la alternativa de Microsoft.

El Ing. Tamayo fue mucho más allá y nos manifestó que el conocía que en el pasado hubo un ingreso ilegal a los servidores de la empresa TV CABLE, y no se pudo hacer nada para contrarrestar el ataque y solamente paso a ser solamente una estadística de los tantos ataques que se dan en el internet.

2.5. Verificación de la Hipótesis

¿El Desarrollo de pruebas de un Servidor Trampa (Honeypot) permitirá garantizar la integridad de la información en una red de comunicación?

Una vez realizada la investigación podemos determinar que mediante la implementación del honeypot si se precautela la información ya que los ataques se lo realizaron a los servidores desprotegidos y no al que contenía toda la información ni a los servidores de DMZ.

Debemos manifestar que también se pudo observar lo importante de saber quienes son los que más atacan ya que no necesariamente son usuarios externos sino más bien los mismos empleados de una institución o empresa los que buscan hacer daño a la información.

El tema trato de ir un poco más allá al realizar una Informática Forense de toda la información que se afecto con los ataques, procedencias al conocer la dirección IP Publica por la que se accedió a nuestra red y servidores.

CAPITULO III

3. DESARROLLAR LAS PRUEBAS DE UN SERVIDOR TRAMPA (HONEYPOT)

Sistema operativo Linux

En este punto de nuestro trabajo de investigación creemos necesario realizar una rápida pero concreta definición del Sistema Operativo Linux y las bondades que este puede brindar a los usuarios de servidores, al tratarse de un Sistema Open Source ha sido ampliamente difundido a nivel mundial por lo que siempre es interesante realizar un análisis.

Linux es probablemente el acontecimiento más importante del software gratuito desde el original Space War, o, más recientemente, Emacs. Se ha convertido en el sistema operativo para los negocios, educación, y provecho personal. Linux ya no es solo para gurus de UNIX que se sientan durante horas frente a sus computadores personales (aunque le aseguramos que un gran número de usuarios pertenece a esta categoría).

Lo que hace a Linux tan diferente es que es una implementación gratuita de UNIX. Fue y aun es desarrollado por un grupo de voluntarios, principalmente en Internet, intercambiando código, comentando fallos, y arreglando los problemas en un entorno abierto. Cualquiera es bienvenido a sumarse al esfuerzo de desarrollo de Linux: todo lo que se pide es interés

en producir un clónico gratuito de UNIX y algunos conocimientos de programación. El presente tema de investigación es una guía que facilitara algunas de las medidas que se deben tomar para garantizar un normal desenvolvimiento de servicios tanto para compartir recursos como para asegurar de manera optima la información de una empresa o institución.

Para entender de mejor manera realizaremos una rápida reseña histórica:

UNIX es uno de los sistemas operativos más populares del mundo debido a su extenso soporte y distribución. Originalmente fue desarrollado como sistema multitarea con tiempo compartido para mini ordenadores y mainframes a mediados de los 70, y desde entonces se ha convertido en uno de los sistemas mas utilizados a pesar de su, ocasionalmente, confusa interfaz con el usuario y el problema de su estandarización.

Linux es una versión de UNIX de libre distribución, inicialmente desarrollada por Linus Torvalds[1] en la Universidad de Helsinki, en Finlandia. Fue desarrollado con la ayuda de muchos programadores y expertos de UNIX a lo largo y ancho del mundo, gracias a la presencia de Internet. Cualquier habitante del planeta puede acceder a Linux y desarrollar nuevos módulos o cambiarlo a su antojo. El núcleo de Linux no utiliza ni una sola línea del código de AT&T o de cualquier otra fuente de propiedad comercial, y buena parte del software para Linux se desarrolla bajo las reglas del proyecto de GNU de la Free Software Foundation, Cambridge, Massachusetts.

[1] torvalds@kruuna.helsinki.fi.

Inicialmente, solo fue un proyecto de aficionado de Linus Torvalds. Se inspiraba en Minix, un pequeño UNIX desarrollado por Andy Tanenbaum, y las primeras discusiones sobre Linux surgieron en el grupo de News comp.os.minix. Estas discusiones giraban en torno al desarrollo de un pequeño sistema UNIX de carácter académico dirigido a aquellos usuarios de Minix que querían algo más.

El desarrollo inicial de Linux ya aprovechaba las características de conmutación de tareas en modo protegido del 386, y se escribió todo en ensamblador. Linus dice, "Comencé a utilizar el C tras escribir algunos drivers, y ciertamente se acelero el desarrollo.

En este punto sentí que mi idea de hacer un `un Minix mejor que Minix' se hacia mas seria. Esperaba que algún día pudiese recompilar el gcc bajo Linux.

"Dos meses de trabajo, hasta que tuve un driver de discos (con numerosos bugs, pero que parecía funcionar en mi PC) y un pequeño sistema de ficheros. Aquí tenía ya la versión 0.01 [al final de Agosto de 1991]: no era muy agradable de usar sin el driver de disquetes, y no hacia gran cosa. No pensé que alguien compilaría esa versión." No se anuncio nada sobre esa versión, puesto que las fuentes del 0.01 jamás fueron ejecutables: contenían solo rudimentos de lo que seria el núcleo, y se asumía que se tenia acceso a un Minix para poderlo compilar y jugar con el.

El 5 de Octubre de 1991, Linus anuncio la primera versión "oficial" de Linux, la 0.02. Ya podía ejecutar bash (el shell de GNU) y gcc (el compilador de C de GNU), pero no hacia mucho mas. La intención era ser

un juguete para hackers. No había nada sobre soporte a usuarios, distribuciones, documentación ni nada parecido. Hoy, la comunidad de Linux aun trata estos asuntos de forma secundaria. Lo primero sigue siendo el desarrollo del kernel.

Linus escribía en comp.os.minix, tras la versión 0.03, Linus salto a la versión 0.10, al tiempo que más gente empezaba a participar en su desarrollo. Tras numerosas revisiones, se alcanzo la versión 0.95, reflejando la esperanza de tener lista muy pronto una versión "oficial". (Generalmente, la versión 1.0 de los programas se corresponden con la primera teóricamente completa y sin errores). Esto sucedía en Marzo de 1992. Año y medio después, en Diciembre del 93, el núcleo estaba en la revisión 0.99.pl14, en una aproximación asintótica al 1.0. Actualmente, el núcleo se encuentra en la versión 1.1 parche 52, y se acerca la 1.2.[2] [2.1]

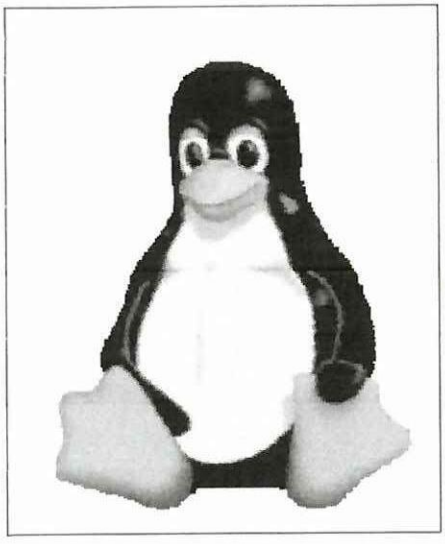
Hoy Linux es ya un clónico de UNIX completo, capaz de ejecutar X Window, TCP/IP, Emacs, UUCP y software de correo y News. Mucho software de libre distribución ha sido ya portado a Linux, y están empezando a aparecer aplicaciones comerciales. El hardware soportado es mucho mayor que en las primeras versiones del núcleo. Mucha gente ha ejecutado tests de rendimiento en sus sistemas Linux 486 y se han encontrado que son comparables a las estaciones de trabajo de gama media de Sun Microsystems y Digital. Quien iba a imaginar que este "pequeño" clónico de UNIX iba a convertirse en un estándar mundial para los ordenadores personales?

[2] En el momento de traducir estas líneas la versión estable del núcleo es la 1.2.13, pero el desarrollo continua por la 1.3.47 en versión beta . . .

[2.1] En estos dias (1999) esta disponible la versión 2.2.7 del Kernel

FIGURA 3.1

REPRESENTACIÓN GRAFICA DEL PROYECTO LINUX



Fuente: Grupo Investigador.(www.linux.org.es)

3.1. FACTIBILIDAD.

3.1.1. Factibilidad Técnica.

El desarrollo de este y cualquier otro proyecto en el cual se va a reforzar las seguridades de un departamento de sistemas, y las seguridades de la información es principalmente influenciado por 3 grandes objetivos los mismos que deben ser cumplidos para poder alcanzar la factibilidad técnica:

- Resolver un problema: Esto es cuando ya existe un servidor implementado ya sea para Proxy o firewall y este tiene procesos que ya no satisfacen el desempeño para lo cual fue creado y es necesario hacerles ciertas modificaciones, en cuanto a seguridades ya que sabemos que nos atacan pero no sabemos quien es o cual es el interés del atacante, y de está manera se hace necesario la implementación de un honeypot para despistar a los hackers y poder investigarlos en la manera de atacarnos.

- Dar respuesta a directivos: Cuando se hacen modificaciones de tecnología de la información y las comunicaciones, se tiene que cumplir con lo deseado por los usuarios de las redes y los servidores e inmediatamente reportar a la gerencia sobre todos estos cambios para que conozcan de nuestro accionar dentro de lo que tiene que ver con las seguridades de la información y del hardware en general.

- Aprovechar una oportunidad: Un cambio ya sea para ampliar o mejorar el rendimiento económico de la empresa y su competitividad, siempre es bien visto de parte de las personas encargadas de la gestión empresarial.

Para alcanzar estos objetivos, las empresas emprenden proyectos por una o más de las siguientes razones: capacidad, control, costo, comunicación y competitividad como se lo menciona dentro del Análisis y diseño de Sistemas de Comunicación y Datos.

Capacidad: Las actividades de la empresa están influenciadas por la capacidad de ésta para procesar transacciones con rapidez y eficiencia. Los sistemas de información mejoran esta capacidad en tres formas estas son:

- Aumento de la velocidad de procesamiento.

- Permiten el manejo de un volumen creciente de transacciones.

- Recuperan con rapidez la información.

Control: La falta de comunicación es una fuente común de dificultades que afectan a todos los que laboran en una empresa. Sin embargo, los sistemas

de comunicación bien desarrollados tratan de ampliar la comunicación y facilitan la integración de funciones individuales.

Aumento de la comunicación: Muchas empresas aumentan sus vías de comunicación por medios de redes.

Costo: Muchas empresas han desaparecido y muchas otras imposibilitadas para alcanzar el éxito debido al poco control sobre los costos o por el total desconocimiento para el control de estos. Los sistemas de información juegan un papel importante tanto con el control como en la reducción de los costos de operación.

Ventaja competitiva: Los sistemas de información y las comunicaciones son un arma estratégica que puede cambiar la forma en como compite la empresa en el mercado. Los sistemas de información y las comunicaciones mejoran la organización y ayudan a la empresa a ser más competitiva. Por lo contrario si los competidores de la empresa tienen sistemas de información más avanzados, entonces los sistemas de información y comunicación pueden convertirse en una desventaja competitiva. Por lo tanto las capacidades de los sistemas de información son una consideración importante al formular la estrategia de la empresa.

Una empresa puede ganar ventaja competitiva a través de su sistema de información y comunicación en cuatro formas diferentes que garantizan la competitividad en el mercado estos son: clientes, competidores, proveedores y servicios.

Todo proyecto de sistemas de comunicación debe ser desarrollado bajo las actividades de un grupo de trabajo que se haga responsable del inicio y culminación del sistema de información.

El grupo de trabajo va a depender de tamaño de acuerdo al proyecto que va a desarrollarse.

Vamos a mencionar los puestos claves de un grupo de trabajo pero podría ser más grande o más pequeño o a veces una sola persona puede desarrollar varios puestos, claro como se dijo anteriormente va a depender de esto el tamaño del proyecto. Por tal motivo solo muestra la apreciación personal de acuerdo a la experiencia profesional que se tiene este tema de investigación.

La seguridad, es un aspecto clave para generar en las empresas y en los consumidores la confianza necesaria para que el comercio electrónico se desarrolle. La necesidad de generar confianza, es especialmente importante debido al hecho de que Internet es una red abierta y a la sensación de inseguridad (quizá a veces excesiva) que este hecho genera en los usuarios.

Sin embargo, la seguridad de la red, en este caso Internet, es solo uno de los factores que intervienen en la seguridad del comercio electrónico en conjunto. Más que de la seguridad del pago, los usuarios empiezan a preocuparse sobre todo de problemas como ¿es el vendedor fiable?, ¿podré devolver el producto si no me gusta?, ¿utilizará mis datos personales para enviarme publicidad que no deseo?, ¿cederá esos datos a otras empresas?, en el caso de empresas ¿cuál es la validez de un pedido, factura, etc. hechos electrónicamente?

Así, aunque las características de seguridad de las redes y sistemas de comercio electrónico son, obviamente, muy importantes, el hecho de que los usuarios consideren el comercio electrónico como suficientemente seguro probablemente depende menos de los detalles técnicos, y más de otras cuestiones como la confianza que inspiren las empresas vendedoras, financieras, etc.; la existencia y difusión de normas que, por ejemplo, limiten la responsabilidad del usuario en caso de uso indebido de una tarjeta de crédito y que garanticen su derecho a devolver un producto comprado electrónicamente; la creación de códigos éticos de comportamiento de las empresas y de procedimientos efectivos de solución de conflictos; etc.

Componentes de seguridad

Las condiciones que debe reunir una comunicación segura a través de Internet (o de otras redes) son en general las siguientes:

- Confidencialidad: evita que un tercero pueda acceder a la información enviada.

- Integridad: evita que un tercero pueda modificar la información enviada sin que lo advierta el destinatario.

- Autenticación: permite a cada lado de la comunicación asegurarse de que el otro lado es realmente quien dice ser.

- No repudio o irrefutabilidad: Permite a cada lado de la comunicación probar fehacientemente que el otro lado ha participado en la comunicación. En el caso de no repudio de origen, el remitente del mensaje no puede negar haberlo enviado.

En el caso de no repudio de destino, el destinatario del mensaje no puede negar haberlo recibido.

La herramienta básica para cumplir las condiciones anteriores son las técnicas criptográficas, en particular los métodos de cifrado simétrico (usan una misma clave secreta para cifrar y descifrar) o asimétrico (cada usuario tiene una pareja de claves, una pública y otra privada, con la propiedad de que lo que se cifra con una de las claves sólo se puede descifrar con la otra). Para evitar posibles suplantaciones de identidad, es necesario contar con una tercera parte fiable que acredite de forma fehaciente cuál es la clave pública de cada persona o entidad. Esta es la función básica de las autoridades de certificación.

Un certificado digital emitido por una de estas autoridades contiene la identidad de un usuario, su clave pública y otros datos adicionales (por ejemplo, el periodo de validez del certificado), todo ello firmado digitalmente con la clave privada de la autoridad de certificación, con el fin de que el certificado no se pueda falsificar. Pueden existir varios tipos de certificados, válidos para diferentes usos, según la información y garantías que la autoridad de certificación (directamente o a través de una autoridad de registro) pide al usuario antes de emitir el certificado.

3.1.2. Factibilidad Económica.

Sin bien es cierto el destinar un equipo o un servidor implica gastos a una empresa o institución, pero de igual manera la momento de asegurar la información nada resulta un gasto sino más bien una inversión.

Que el peligro está ahí fuera y que todo sistema es susceptible de ser atacado, es algo que se ha empezado a asumir en la comunidad virtual.

¿Qué mejor que admitirlo y aprovecharse de esta circunstancia?. Los honeypots son un nuevo concepto en herramientas de seguridad que ayudan a entender, rastrear e investigar ataques realizados a través de Internet. La definición más acertada puede ser un sistema diseñado para ser atacado, probado o comprometido, al que se hace más atractivo gracias a pequeños señuelos o cebos que atraigan a hacker.

Siguiendo la analogía que le ha dado nombre, los hackers son las moscas, atraídas por la dulce miel (el sistema) que se les presenta, pues se les hace creer que contiene algún secreto oculto, ya sean contraseñas, datos o la posibilidad de ganar el control de la máquina. Pero todo esto es ilusorio, porque ante un honeypot, el cazador se convierte en víctima y lo que realmente se espera del hacker es precisamente esto, que caiga en las redes de una presunta víctima fácil y comience a demostrar sus mejores artes.

¿Para qué? La respuesta es sencilla.

De esta manera se puede estudiar su comportamiento, deducir las prácticas más habituales, descubrir nuevos exploits, rastrear sus pasos en definitiva, estudiar sus movimientos para analizarlos posteriormente. Y, de paso, mantener entretenido al pirata y ocupado en sistemas que no corren ningún peligro mientras se mantiene a salvo los verdaderos servidores importantes.

Un honeypot puede ser tan simple como un ordenador que ejecuta un programa escuchando en cualquier número de puertos. Al programa, al sistema operativo, al protocolo o a cualquier otro elemento de la cadena se le mantiene una vulnerabilidad o debilidad que lo haga más goloso y cree confianza en el pirata, de manera que se muestre dispuesto a emplear todas sus habilidades para explotarlo y ganar acceso al sistema.

Por otro lado, un honeypot puede ser tan complejo como una completa red de ordenadores completamente funcionales corriendo bajo distintos sistemas operativos y ofreciendo gran cantidad de servicios, y hacer que cuando alguna computadora que lo comprende sea escaneada, se advierta al administrador mediante email, SMS o cualquier otro sistema de alerta.

Pero también puede ser todo virtual, los hay ya listos para ser usados, programas específicamente diseñados para simular una red, engañar al pirata con direcciones falsas, IP fingidas y ordenadores inexistentes, con el único fin de confundir al hacker creyendo que ha entrado y tiene acceso a una red inmensa donde, con toda probabilidad, habrá un montón de miel lista para ser probada. Pero se equivoca, si algo tienen en común los *honeypot*s es que no guardan ninguna información relevante, y si lo parece, (si se muestran contraseñas o datos de usuario) son completamente ficticios.

Por último, se puede construir uno mismo un *honeypot* artesano, hecho a mano, abriendo pequeñas brechas de seguridad a conciencia y teniendo en cuenta hasta el último detalle. Esto se hace, en general, para comprobar qué clase de motivaciones atraen más a los atacantes, no sólo humanos, también se puede estudiar el comportamiento de un gusano o virus que se conoce ataca una vulnerabilidad concreta.

Preparar un ordenador tarado con esa vulnerabilidad y diseñar en sus "bambalinas" todo un sistema de alerta y rastreo que registre paso a paso la actividad del gusano puede ser gran utilidad a la hora de programar una vacuna y, en definitiva, "conocer al enemigo".

En conclusión: A medida que la seguridad parece empezar a preocupar más y más a los especialistas, convirtiéndola en la base crítica en la que se sustentan todos los proyectos dedicados en la red, los *honeypots* (literalmente, tarros de miel) han ganado en popularidad y aceptación, presentándose como una herramienta eficaz y poderosa ante los temidos hackers. Ya lo aventuraba Samaniego allá por el siglo XVIII: "A un panal de rica miel / dos mil moscas acudieron / y por golosas murieron / presas de patas en él".

3.1.3. Factibilidad Operacional.

Lance Spitzner es un consultor y analista informático experto en temas de seguridad. Construyó a comienzos de 2000 una red de seis ordenadores en su casa diseñada para estudiar el comportamiento y formas de actuación de los hackers. Fue de los primeros en adoptar la idea, hoy es uno de los mayores expertos en *honeypots*, precursor del proyecto honeynet (project.honeynet.org), en marcha desde 1999 y autor del libro "Honeypots: Tracking Hackers".

Su sistema estuvo en marcha durante casi un año de prueba, desde abril del 2000 a febrero de 2001, guardando toda la información que se generaba. Los resultados hablaban por sí solos: en los momentos de más intensidad, comprobaban que las vías de acceso más comunes eran comprobadas

desde el exterior hasta 14 veces al día, con herramientas de ataque automatizadas.

Su utilidad es más que interesante. Los *honeypot*s se usan para mitigar los riesgos de las compañías, en el sentido tradicional de uso de las conocidas herramientas defensivas. Lo que la diferencia de los típicos firewalls o detectores de intrusos es su naturaleza "activa" en vez de pasiva. Se muestra como un anzuelo, no como un muro de contención para evitar ataques, muy al contrario, los busca y se encarga de "entretenerlos".

Muchas compañías lo usan como un valor añadido más a sus elementos de seguridad, como complemento a sus herramientas típicas, buscando la fácil detección y reconocimiento de los ataques, de manera que puedan elaborar con esos datos estadísticas que ayuden a configurar de manera más efectiva sus herramientas pasivas. Conociendo los problemas de seguridad a los que más ataca la comunidad hacker, más eficazmente podrá defenderse una compañía concreta contra ellos.

Sus ventajas e inconvenientes

Como toda herramienta destinada mejorar la seguridad, los *honeypot*s tienen sus ventajas e inconvenientes. Su mayor utilidad radica en su simpleza. Al ser un mecanismo cuyo único fin consiste en que intenten abusar de él, no realiza ningún servicio real, y el tráfico que transita a través de él va a ser muy pequeño.

Si se detecta tráfico que va o viene hacia el sistema, casi con toda probabilidad va a ser una prueba, escaneo o ataque. El tráfico registrado en

un sistema de este tipo es sospechoso por naturaleza, por lo que su gestión y estudio se simplifica en gran medida. Aunque, por supuesto, ocurran "falsos positivos", expresión que, en este caso, invierte su significado. Si un falso positivo se produce normalmente cuando una actividad sospechosa tomada como ataque no resulta serlo, en el ambiente de los "tarros de miel", el falso positivo sería el tráfico gestionado por la máquina que no representa una amenaza. En esta simpleza de uso de tráfico y recursos, radica su mayor ventaja. En resumen, poca información, pero muy valiosa.

Entre los problemas que puede causar, destaca la posibilidad de que se vuelva en nuestra contra. Si no se diseña de una manera absolutamente estudiada, si no se ata cada cabo, el pirata puede acabar llevándose el cebo sin ser atrapado por la caña. Si descubre alguna otra vulnerabilidad no prevista o consigue burlar los sistemas de registro, puede usar el ordenador atacado como plataforma para otros ataques o, lo que representaría un completo fracaso del sistema, comprometer máquinas reales con datos valiosos conectados al *honeypot*.

Los hackers no son estúpidos, saben que existen herramientas destinadas para darles caza, y antes de dejarse llevar ante una víctima, realizan varias comprobaciones "rutinarias" que les ayudan a conocer a qué tipo de sistemas se están enfrentando. Esto puede ser un problema para los tarros de miel. Por ejemplo, un *honeypot* puede estar diseñado para emular un servidor web IIS bajo Windows 2000, pero correr bajo un servidor Unix Solaris. Hay gran variedad de métodos para que el propio servidor nos comunique algunas pistas de lo que es y qué contiene. Si se llega a averiguar esta contradicción, el pirata sospechará enseguida y abandonará el sistema sin realizar más ataques.

Investiga a tu enemigo: Construyendo Honeynets

Honeynet es el nombre que se le ha dado al tipo de honeypot específicamente diseñado para la investigación. Si los *honeypot*s pueden ser usados por una empresa privada para detectar ataques de manera más fácil, rápida y efectiva, en vez de tener que desenvolverse entre gigas y gigas de logs almacenados, las honeynet tienen el propósito principal de investigar el uso de las técnicas y herramientas que hacen los chicos malos de Internet.

Se diferencia básicamente en que no supone una sola máquina, sino múltiples sistemas y aplicaciones que emulan otras tantas, imitan vulnerabilidades o servicios conocidos o crean entornos "jaula" donde mejor observar los ataques.

Los requerimientos básicos e imprescindibles para construir una *honeynet* son: Data Control (control de datos) y Data Capture (captura de datos).
Los Data Control suponen la contención controlada de la información y las conexiones. Lidiar con hackers siempre supone un riesgo que hay que reducir al máximo, por lo que es preciso asegurarse que una vez comprometido el *honeypot*, no se comprometerán sistemas legítimos. El reto consiste en mantener un absoluto control del flujo de datos sin que el pirata lo note. No se puede cerrar un sistema por completo para evitar el tráfico innecesario. Una vez comprometido el sistema, el hacker intentará realizar distintos tipos de conexiones para continuar su ataque, probablemente necesite bajar programas por ftp, correo o conexiones SSH.

Si no se le permite esta flexibilidad de acciones, además de levantar sus sospechas, no se podrán estudiar uno de los pasos más importantes que

valdría la pena analizar. En los primeros intentos de los investigadores de poner en marcha proyectos de *honeynet*, no se permitieron ningún tipo de conexiones salientes para evitar ser plataforma de nuevos ataques. Pero sólo les llevaba a los atacantes unos diez minutos ver que algo andaba mal, y abandonar el intento de ataque. Los resultados así eran muy pobres. De esto se deduce una disyuntiva en la que reside el arte de una buena red de miel.

Es necesario encontrar el equilibrio entre la libertad de movimientos para el hacker, que supone un mayor riesgo, y la seguridad real del sistema, que puede derivar en resultados menos interesantes para el estudio.

El otro punto fuerte de las *honeynets* es el Data Capture, o el rastreo y almacenamiento de la información que perseguimos, o sea, los logs de sus actos que serán analizados a posteriori. Se debe capturar tanta información como sea posible aislada del tráfico legal, evitando la posibilidad de que el hacker sepa que se le está "grabando en vivo". Lo más importante para conseguir esto, es no guardar los resultados localmente en el *honeypot*, pues pueden ser potencialmente detectados y borrados con la lógica intención de no dejar huellas del ataque. La información debe ser almacenada remotamente y en capas. No se puede limitar al registro de una simple capa de información, sino tomarla de la mayor variedad posible de recursos. Combinándolos, las capas formarán el cuadro deseado.

Soluciones completas o "hágalo usted mismo"

A nivel software, existen innumerables herramientas en Internet para llevar a cabo el proyecto. Brian Pontz ha programado una serie de parches para el

kernel de sistemas Linux que registra transparentemente todas las pulsaciones de teclado.

Se pueden encontrar en http://www.axehind.com/honeynet/. Si la plataforma es Windows, el programa Winetd, descargable desde ttp://www.cotse.com/CotseLabs/winetd/ puede simular servicios inetd de los sistemas Linux. Acaba de salir "al mercado", un conjunto de herramientas gratuitas creadas por Marcus Ranum y Lnace Spitzner que contienen ficheros de configuración, binarios precompilados y scripts para construir tu propia *honeypot* en segundos bajo Linux.

Descargable desde http://www.tracking-hackers.com/solutions/kit.tgz Se pueden encontrar soluciones completas tanto comerciales como en el ámbito del código abierto.

Merece la pena nombrar las capacidades de algunos de ellos.

Specter (http://www.specter.com), que funciona bajo Windows, es una solución de pago que puede emular trece sistemas operativos distintos, monitorizar hasta catorce puertos TCP y otras muchas funcionalidades. Su mejor baza es la facilidad de uso.

Para entrenar gratuitamente, podemos empezar con Tiny *Honeypot*, (http://www.alpinista.org/thp) escrita por George Bakos y la única que siempre se muestra vulnerable cualquiera que sea el tipo de ataque que efectúe el hacker. La mejor para coleccionar gran cantidad de herramientas y costumbres de los hackers.

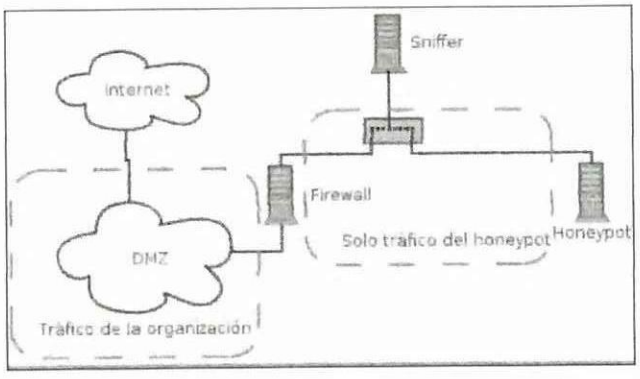
3.2. DISEÑO FÍSICO DE LAS REDES PLANTEADO, PARA GARANTIZAR SEGURIDADES CON UN SERVIDOR TRAMPA.

3.2.1. Acceso ilimitado a Internet.

La configuración de Internet en una red de área local está dada por el numero de usuarios, las actividades que van a realizar los usuarios, si la información que se ingresa en un sistema utiliza VPN o se encuentra abierta dentro del Internet.

Así podemos observar en el grafico siguiente:

FIGURA 3.2
DISEÑO DEL HONEYPOT EN UN SERVIDOR DE DMZ A INTERNET



Fuente: Grupo Investigador (www.linuxparatodos.com)

Como se puede dar la administración del tráfico de Internet cuando esta cuenta con un *DMZ* para la administración WEB esto es correo electrónico, pagina web, se tiene abierto el ftp, para la descarga de archivos de los distintos sitios web.

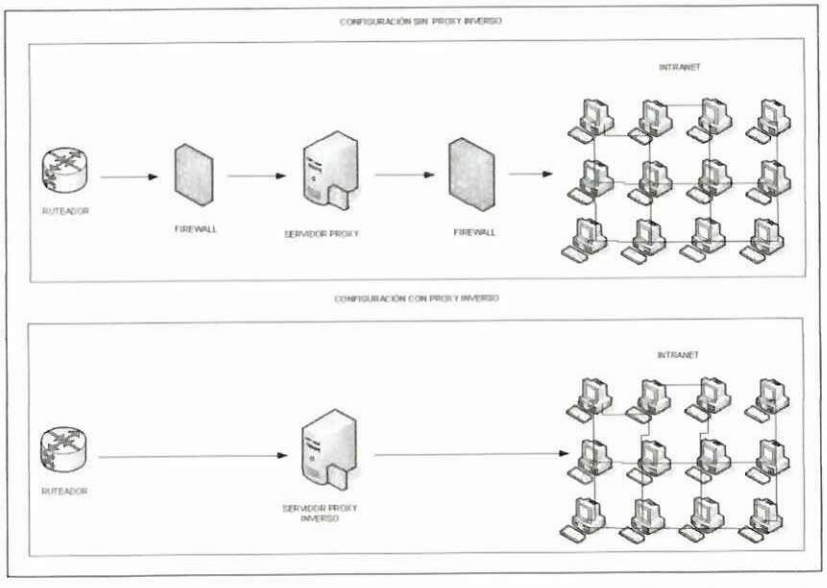
Siempre debemos tener configurado el firewall ya que esto es llama la atención a un hacker, tratar de vulnerar las seguridades de una red que tiene un firewall es porque tiene información importante o valiosa para toda empresa o institución.

3.2.2. Acceso limitado a Internet.

Cuando deseamos tener un acceso ilimitado a Internet podemos tomar en cuenta lo más general son el proveedor de servicios de Internet uno o dos firewalls dependiendo del número de usuarios, el tipo de información que se maneje dentro de una empresa o institución.

FIGURA 3.3

CONFIGURACIÓN DE SERVIDORES PROXY PARA ACCESO A INTERNET



Fuente: Grupo Investigador

Como podemos observar en la grafica tenemos dos alternativas de acceso al recurso de Internet ilimitado sin necesidad de contar con un honeypot ya que este solamente seria un recurso de distracción que no cumpliría ningún

papel al momento de entregar la información o el recurso de internet dentro de la empresa.

3.3. IMPLEMENTACIÓN DE SEGURIDADES LÓGICAS MEDIANTE HONEYPOT

3.3.1. Local.

Para poder tener un sistema 100% seguras hay que tomar en cuenta algunos estándares que garanticen el buen funcionamiento de lo servidores. Partiendo de estos principios se hace necesaria la correcta implementación de los servidores, partiendo desde su instalación misma tomando en cuenta por ejemplo:

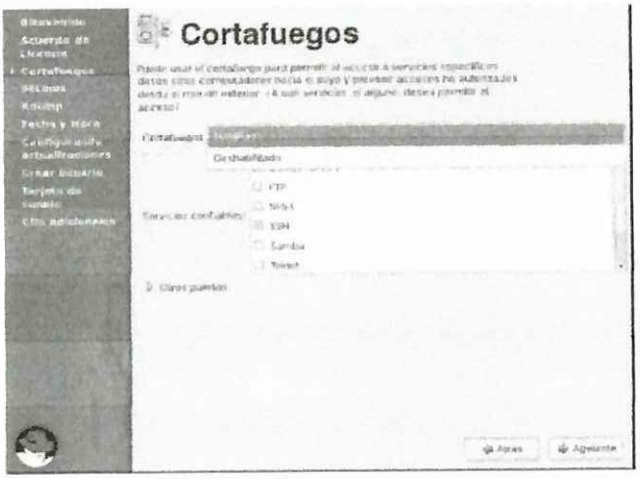
FIGURA 3.4
INSTALACIÓN SEGURA DE SERVIDORES

Fuente: Grupo Investigador

En la grafica nos muestra como se instala un servidor normalmente, tomando en cuenta que todos los servicios que se instalan son puertos abiertos y potencialmente serian puertas de ingreso para atentar contra la información de una empresa o institución.

FIGURA 3.5

INSTALACIÓN DEL FIREWALL MEDIANTE ASISTENTES



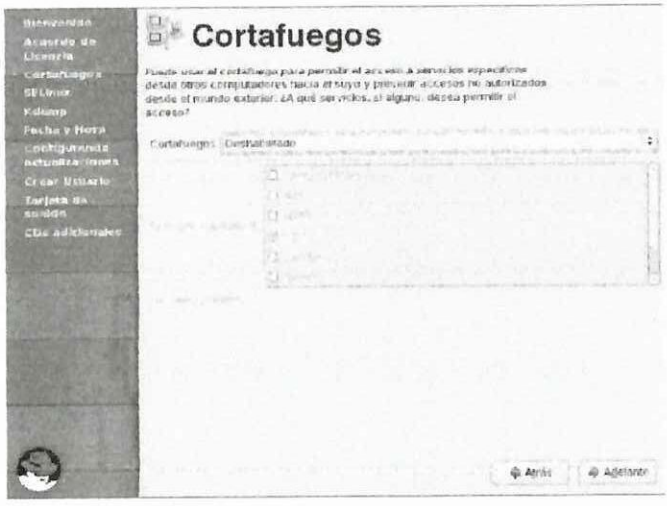
Fuente: Grupo Investigador

La implementación de un Firewall es un proceso muy delicado ya que contiene muchas alternativas y si las ponemos por defecto las que nos vienen en la instalación filtra demasiado o simplemente no filtra lo que se desea que se filtre, y resulta una carga por el recurso que consume un Cortafuegos en un sistema Operativo sea este de Microsoft o de Open Source como el Linux.

Hay que tomar en cuenta que el Linux casi siempre deja abierto el puerto del SSH que es para comunicación remota segura. Como se puede notar en la grafica anterior.

FIGURA 3.6

DESACTIVACIÓN DEL FIREWALL



Fuente: Grupo Investigador

Como se mencionaba en la parte superior de la investigación es necesario la implementación de un firewall, y para nuestro tema de investigación hemos tomado en cuenta la configuración por defecto de un firewall en el servidor de Linux Red Hat 5, sin embargo como se puede ver en la grafica al momento de desactivar la opción de Firewall todos los recursos especialmente del *DMZ* quedan desprotegidos.

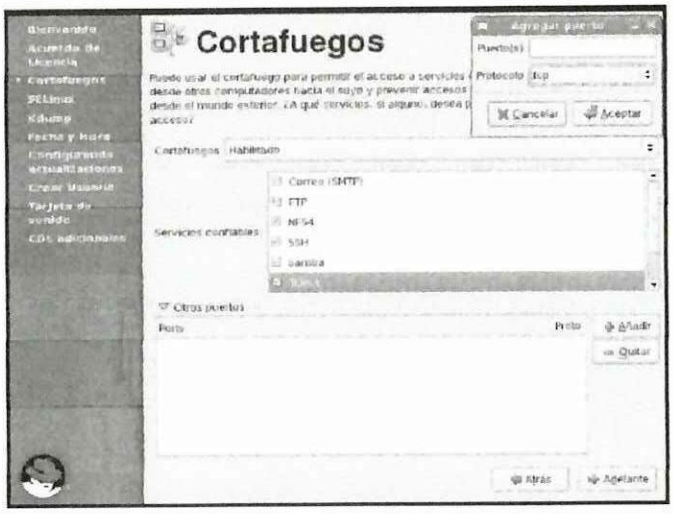
3.3.2. Externa.

Para la configuración del Firewall del modo externo debemos tener muy en cuenta su configuración mediante los IPTABLES ya que de está manera se garantiza toda la información que tiene la red empresarial, no obstante la configuración de los IPTABLES debe garantizar que no solamente fluya información dentro de una red sino que se precautele la misma.

La opción mas recomendada para la implementación de un HONEYPOT es la siguiente:

FIGURA 3.7

CONFIGURACIÓN DE UN SERVIDOR SIN SEGURIDADES



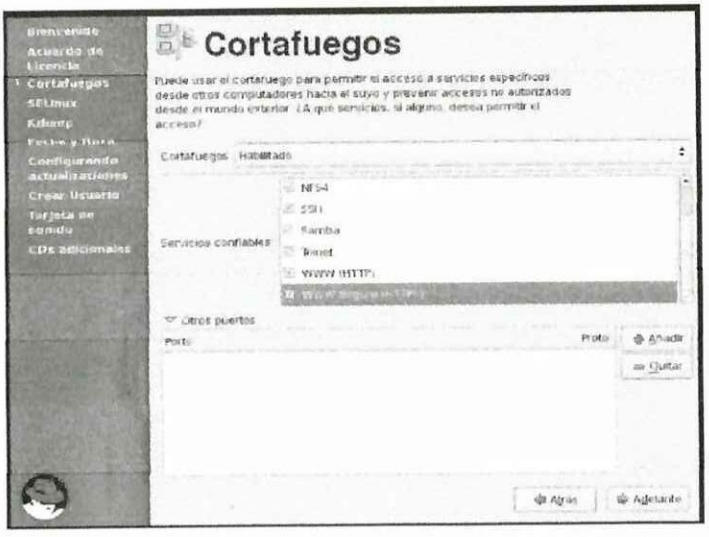
Fuente: Grupo Investigador

Como se puede observar abrimos la mayor cantidad de puertos posibles incluyendo todos los DMZ, además de los puertos de administración remota, que son los que más rastrean las personas mediante herramientas de snnifer.

Otras de las características a tomar en cuenta es la apertura de puertos de http y https, ya que esto significa que una empresa cuenta con la infraestructura necesaria para tener un sitio web y si este sitio es seguro la información que por está circula cuenta con una firma digital.

FIGURA 3.8

ACTIVACIÓN DE PUERTOS PARA ADMINISTRACIÓN DE PÁGINAS WEB



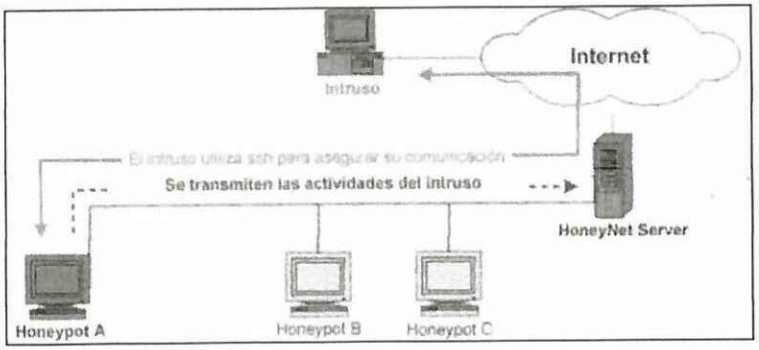
Fuente: Grupo Investigador

3.4. EMULACIÓN DE SERVICIOS.

Para la emulación de varios honeypot podemos gráficamente detallar de la siguiente manera:

FIGURA 3.9

SIMULACIÓN GRAFICA DE VARIOS HONEYPOT



Fuente: Grupo Investigador

Como se puede observar en la gráfica anterior tenemos un equipo que intenta vulnerar las seguridades de algunos de nuestros servidores pero la

única oportunidad de acceso es mediante el SSH que es un servicio de administración remota como el Telnet la diferencia es que este tiene algunas características de seguro y garantiza la información que se envía y recibe.

Lo que más importa en este ejemplo es que tenemos 3 servidores trampa además de una red trampa la misma que desvía la atención de los hackers o de los mismos virus que intentan atacar posibles vulnerabilidades.

3.5. Emulación de Puertos Abiertos.

Existen algunas alternativas de rastreo de puertos la más utilizada es mediante el tomando nmap quien se encarga de rastrear de forma automática todos los puertos abiertos que tienen por ejemplo:

FIGURA 3.10

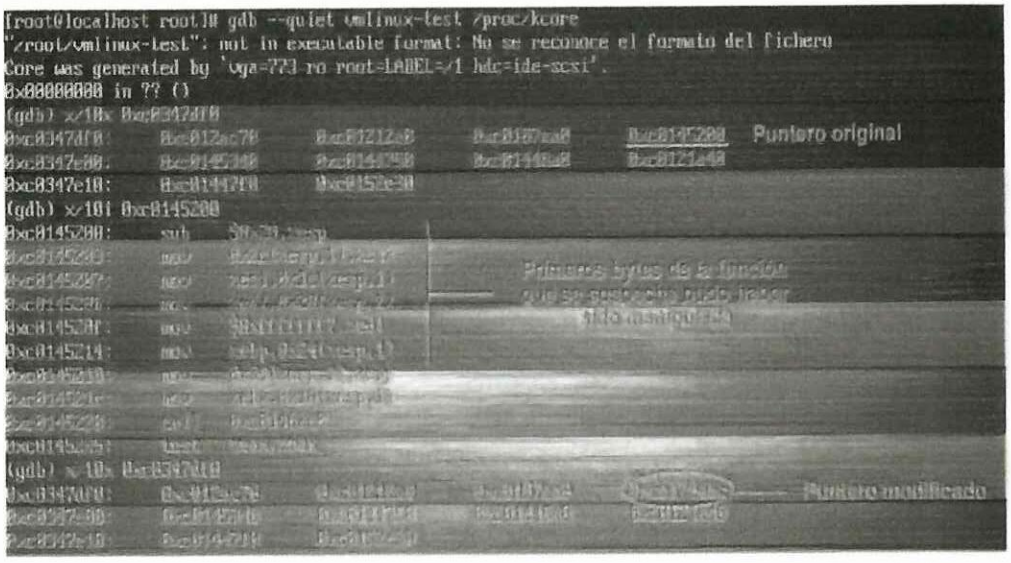
SCANNER DE PUERTOS EN LINUX

Fuente: Grupo Investigador

Pero lo que deberás importa al momento de las configuraciones de un Honeypot es ver quienes son los potenciales atacantes y esto lo hicimos mediante código de Linux el mismo que detallamos:

FIGURA 3.11

SCANNER DE PUERTOS EN UN HONEYPOT



Fuente: Grupo Investigador

Aquí podemos observar como nos dan las direcciones de memoria ante posibles ataques, así como podríamos matar algunos procesos muertos que estén dentro de nuestro honeypot que no seria lo ideal sino más bien estudiarlos para ver que les interesa de nuestro servidor.

3.6. Principios Básicos de la Informática Forense.

El tema de la **Informática Forense** fue expuesto en el Boletín de Seguridad Informática de septiembre de 2003 publicado por la Asociación Bancaria, el cual se define como la aplicación de técnicas y herramientas de hardware y software orientados a analizar sistemas informáticos en busca de evidencia que colabore a llevar adelante una causa judicial o una negociación extrajudicial.

En dicho boletín se menciona la variedad de aplicaciones de la informática forense dado el creciente uso de la tecnología en la operación cotidiana de

las empresas de los diversos sectores, entre ellos por su supuesto, el financiero.

Por lo anterior y teniendo presente aspectos ya mencionados en el boletín, tales como: principios para el manejo, recolección y recuperación de evidencia digital, herramientas para la investigación forense, pasos para el estudio forense y las dificultades que podría tener el investigador forense, en este documento trataremos lo que podría ser en la práctica una investigación forense de un caso en el sector financiero tomando como ejemplo una transacción típica de la operación bancaria.

En la investigación forense existe una gran debilidad: frente a la evidencia documental, la evidencia digital es frágil, dado que la copia de un documento almacenado en un archivo es idéntica al original. Asimismo, existe el riesgo potencial de realizar copias no autorizadas del archivo original sin que quede evidencia de dicha acción. Por lo anterior, en este tipo de investigaciones se deben cumplir con los principios que citamos a continuación:

Sugerencias para luego de utilizar un Honeypot.

a. Durante el proceso de recolección de evidencia digital, la evidencia no debe sufrir ningún cambio.

b. Cuando se requiere que una persona tenga acceso a evidencia digital original, dicha persona debe ser un profesional forense.

c. Toda actividad referente a la recolección, el acceso, el almacenamiento o la transferencia de la evidencia digital, debe ser documentada completamente, preservada y disponible para revisión.

d. Mientras la evidencia digital esté en poder de un individuo, éste será totalmente responsable de las acciones tomadas con la misma.

e. Cualquier entidad que sea responsable de recolectar, almacenar o transferir evidencia digital es responsable de cumplir con estos principios.

f. Durante todo el proceso de recolección de evidencia digital, debe haber testigos que certifiquen los procedimientos efectuados.

En cuanto al proceso de recuperación, se debe cumplir como mínimo con 4 aspectos fundamentales: capacidad para brindar confianza en cuanto a la integridad de la evidencia, uso de un lenguaje sencillo, aplicabilidad a toda la evidencia forense y ser consistente con todos los sistemas legales.

En lo referente a las **herramientas para la investigación forense**, existe una gran variedad y dependen del objetivo para la cual van a ser utilizadas. Existen para la recolección de evidencia (las de mayor importancia en la computación forense), para el monitoreo o control de computadores, para el marcado de documentos y de hardware (dispositivos físicos para la recolección de evidencia). Ahora, toda investigación forense en términos generales involucra como mínimo para su desarrollo **cuatro pasos** que enunciamos a continuación:

a. Preparación y conocimiento general.
b. Recolección y manipulación.

c. Inspección y análisis de la evidencia.
d. Reconstrucción de los hechos.

Finalmente, en cuanto las **dificultades** que podría tener el investigador forense, se relacionan con factores como su habilidad, experiencia, carencia de herramientas especializadas, deficientes o inexistentes rastros de auditoria o resistencia por parte de algunos funcionarios de la entidad para la entrega o dar acceso a la información de la entidad (en la exposición del caso, se presenta de manera práctica esta problemática).

Dentro de nuestra investigación hemos podido encontrar muchas herramientas que luego de los ataques de los hacker y la detección por medio de un HONEYPOT han entrado en práctica algunas herramientas de hardware:

El proceso de recolección de evidencia debe ser lo menos invasivo posible con el objeto de no modificar la información. Esto ha dado origen al desarrollo de herramientas que incluyen dispositivos como conectores, unidades de grabación, etc. Es el caso de herramientas como DIBS "Portable Evidence Recovery Unit" y una serie de herramientas de Intelligent Computer Solutions; LinkMASSter Forensic Soft Case, LinkMASSter Forensic Hard Case, Image MASSter Solo 2 Forensic Kit With Hard Case.

Asimismo, debido a la vulnerabilidad de la copia y modificación de los documentos almacenados en archivos magnéticos, los investigadores deben revisar con frecuencia que sus copias son exactas a las del disco del

sospechoso y para esto utilizan varias tecnologías como checksums o Hash MD5.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. Un *Honeypot* puede ser tan simple como un ordenador que ejecuta un programa escuchando cualquier número de puertos.

2. Por otro lado, un *honeypot* puede ser tan complejo como una completa red de ordenadores completamente funcionales corriendo bajo distintos sistemas operativos y ofreciendo gran cantidad de servicios, y hacer que cuando alguna computadora que lo comprende sea escaneada, se advierta al administrador mediante email, SMS o cualquier otro sistema de alerta.

3. Linux Red Hat Enterprise 5 es un sistema operativo que nos permite administrar de mejor manera los servicios de una red, y es tan flexible que permite la ejecución de comandos tan complejos como los de *Honeypot*.

4. Se debe tomar siempre en cuenta los estándares y normas internacionales para la configuración y administración de ciertos servicios con que cuentan los servidores, ya que de está manera estaremos precautelando la información que se genera en los distintos departamentos.

5. El continuo avance de las tecnologías ha influenciado notablemente en la reestructuración de los estándares de la IEEE y de las normas ISO y dentro de estos se ha implementado el Código de Practica para la Administración de la Seguridad de la Información.

6. La norma ISO IEC 17799 manifiesta que la información al igual que el resto de activos de una empresa necesita de todas las seguridades

posibles, razón por la cual invita a seguir algunos pasos para cuidar de ésta.

7. Los servidores deben contar con la mayor cantidad de memoria posible, capaz de garantizar un optimo rendimiento de los sistemas operativos que se ejecuten en las maquinas virtuales, así como un espacio en disco que pueda brindar un trabajo holgado al sistema operativo invitado.

8. La falta de documentación depurada del funcionamiento de los Honeypots y su configuración para ciertos servicios puede confundir a los administradores de los servidores al momento de existir un inconveniente al cual se necesita dar solución de la manera más óptima.

RECOMENDACIONES

1. Hay que manejarlas con mucha prudencia, ya que son herramientas que ayudan a la configuración de equipos hijos, tomando las características de la maquina host y mermando el rendimiento de ésta.

2. La adquisición de equipos sean estos servidores o equipos personales se lo debe realizar buscando cumplir con las expectativas de la empresa o institución donde se vaya a implementar los servidores.

3. Los servidores establecidos en toda empresa son los necesarios en la actualidad pero para un futuro con el crecimiento se debería pensar en incrementar muchos más recursos sobre todo para fomentar la investigación como es los HONEYPOT pero de una manera controlada y no excediendo las especificaciones técnicas de cada equipo.

4. Los estándares aplicados en este proyecto de tesis están siempre en actualización por lo cual no se debe dejar de revisar dichas actualizaciones y aplicar a la institución donde se lo implemente para poder dar un mejor servicio a los usuarios y para mantener un mejor control sobre estos.

5. Se recomienda la capacitación en el manejo del software de todo el hardware que se vaya a incorporar en los servidores para una correcta Gestión de la Red para tener un método más eficiente de los usuarios y los puntos de red para poder dar solución a los inconvenientes propios de la red.

6. Para evitar conflictos de incompatibilidad de equipos de red y otros problemas se recomienda se tome como política de equipos con

recursos suficientes a fin de evitarnos contratiempos en las configuraciones.

7. Se debe pensar ya en la adquisición de nuevos equipos con al menos tres tarjetas de red dos microprocesadores y al menos 4Gb de RAM, para suplir las necesidades existentes en toda institución.

8. Se debe fomentar la investigación en todo sentido ya que el vertiginoso avance tecnológico así lo demanda.

GLOSARIO DE TÉRMINOS Y SIGLAS

Acceso Físico

Es el medio utilizado para obtener información de las oficinas, salas de cómputo, escritorios y archivos.

Acceso Lógico

Es el medio utilizado para obtener información de las bases de datos y sistemas de información de la organización.

Activos

Son los recursos de la organización. Existen varios tipos de activos como son: Los recursos de información (bases de datos, los documentos de sistemas), los recursos de software (software de sistemas operativos, herramientas de desarrollo), activos fisicos (equipamiento informático, equipos de comunicaciones, otros) y servicios (iluminación, energía eléctrica, etc.)

Amplitud de banda

La amplitud de banda especifica la cantidad de datos que pueden transmitirse en una cantidad de tiempo fija. En el caso de los dispositivos digitales, la amplitud de banda se define en bits por segundo (bps) o bytes por segundo.

Anomalía

Irregularidad en el funcionamiento de un sistema, de un software, de un control, etc.

Asic

Circuito integrado específico de una aplicación. Chip personalizado diseñado para una aplicación específica.

Asignaciones de amplitud de banda

La cantidad de amplitud de banda asignada a una aplicación, usuario o interfaz específicos.

Camino Forzado

Ruta limitada entre una Terminal de usuario y los servicios del computador. Evita que los usuarios seleccionen rutas fuera de la trazada entre su Terminal y los servicios a los cuales esta autorizado a acceder.

Canal Oculto

Es un cauce de comunicación que permite a un proceso receptor y a un emisor intercambiar información de forma que viole la política de seguridad del sistema; esencialmente se trata de un método de comunicación que no es parte del diseño original del sistema pero que puede utilizarse para transferir información a un proceso o usuario que a priori no estaría autorizado a acceder a dicha información.

Class of Service (Clase de servicio)

La clase de servicio es el esquema de prioridad 802.1p. La CoS proporciona un método para asignar etiquetas a los paquetes con información sobre la prioridad. Un valor de CoS situado entre 0 y 7 se agrega al encabezado de la capa 2 de los paquetes, donde cero es la prioridad más baja y siete es la más alta.

Transmisión de superposición de dos o más paquetes que colisionan. Los datos transmitidos no pueden utilizarse, y la sesión se reinicia.

Clave Pública

Clave que puede ser revelada a cualquier persona.

Clave Secreta

Clave que debe mantenerse en secreto.

Código Troyano

Es un programa que llega al ordenador de manera encubierta, aparentando ser inofensivo, se instala y realiza determinadas acciones que afectan a la confidencialidad del usuario afectado.

Comercio Electrónico

Consiste en la compra, venta, marketing y suministro de información complementaria para productos o servicios a través de redes informáticas.

Computación Móvil

Se define como la serie de artefactos y equipos portátiles, hardware, que hacen uso de la computación para lograr su funcionamiento, así, se tiene a las computadoras portátiles, los teléfonos celulares, los cuadernos de notas computarizados, las calculadoras de bolsillo, etc.

Capa 2

Capa de vínculo de datos o capa MAC. Contiene la dirección física de un cliente o estación de servidor. El proceso de la capa 2 es más rápido que el de la capa 3 porque hay menos información que deba procesarse.

Capa 4

Establece una conexión y garantiza que todos los datos lleguen a su destino. Los paquetes inspeccionados en el nivel de la capa 4 se analizan y las decisiones se reenvían en función de sus aplicaciones.

Capa MAC

Subcapa de la capa de control de vínculo de datos (DTL).

Criptografía

Dícese de la ciencia que estudia la forma de codificar y descodificar documentos, de forma que sólo puedan ser leídos por la persona que posee la clave de descodificación.

Dirección IP

Dirección del protocolo de Internet. Dirección exclusiva asignada a un dispositivo de red con dos o más LAN o WAN interconectadas.

Dirección MAC

Dirección Media Access Control. La dirección MAC es una dirección específica del hardware que identifica cada nodo de red.

DSCP

DiffServe Code Point (DSCP). DSCP proporciona un método de asignación de etiquetas de paquetes IP con información de prioridad QoS.

Evaluación de Riesgos

Es un proceso dirigido a estimar la magnitud de aquellos riesgos que no hayan podido evitarse, obteniendo la información necesaria para que el empresario esté en condiciones de tomar una decisión apropiada sobre la necesidad de adoptar medidas preventivas y, en tal caso, sobre el tipo de medidas que deben adoptarse. La evaluación de riesgos consta de una fase llamada de análisis de riesgos (identificación de peligros y estimación de los riesgos) y una fase posterior de valoración de riesgos y de control de riesgos si fuese posible.

Evidencia

Datos, registros, declaraciones de hecho o cualquier otra información que respaldan la existencia o veracidad de algo.

Honeypots (Tarro de Miel)

Recurso de red destinado ha ser atacado o comprometido. Los Honeypots son los encargados de proporcionar información valiosa sobre los posibles atacantes en potencia a nuestra red antes de que comprometan sistemas reales. Es decir el objetivo de los Honeypots es recibir los ataques, no recoger información para demandar a los atacantes del Honeypot.

Honeynets (Tarro de Miel)

Es un tipo de Honeypot. Específicamente es un Honeypot altamente interactivo diseñado para la investigación y la obtención de información sobre atacantes. Un Honeynet es una arquitectura, no un producto concreto o un software determinado. Y consiste no en falsear datos o engañar a un posible atacante (como suelen hacer algunos Honeypot), sino que el objetivo principal es recoger información real de cómo actúan los atacantes en un entorno de verdad.

Incidente

Dícese del fallo que sucede en un equipo o sistema de manera temporal o aleatoria, sin que existan unos motivos claros para ello.

Procesamiento de Información

Es la capacidad del Sistema de Información para efectuar cálculos de acuerdo con una secuencia de operaciones preestablecida.
Estos cálculos pueden efectuarse con datos introducidos recientemente en el sistema o bien con datos que están almacenados.

Seguridad Informática

Conjunto de técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionales. Estos daños incluyen el acceso a bases de datos de personas no autorizadas, el mal funcionamiento del hardware y la perdida física de datos.

Seguridad de la Información

La seguridad de la información consiste en proteger uno de los principales activos de cualquier empresa: la información. La seguridad de la información es requisito previo para la existencia a largo plazo de cualquier negocio o entidad. La información es usada en cada uno de los ámbitos empresariales, los cuales dependen de su almacenamiento, procesado y presentación.

Servicio de Información

Un servicio para los sistemas que proporciona un sistema de base de datos para los archivos de configuración comunes.

Servicio de Red

Es un servicio para que cualquier máquina de la red puede comunicarse con otra distinta y esta conectividad permite enlazar redes fisicamente independientes.

Sistema de Información

Conjunto de elementos, ordenadamente relacionados entre sí que aporta al sistema objeto, es decir, a la organización a la cual sirve y le marca directrices de funcionamiento, la información necesaria para el cumplimiento de sus fines, para lo cual tendrá que recoger, procesar y almacenar la información, facilitando la recuperación de la misma.

Sistema Informático

Es aquel sistema que se encarga del manejo de información en la computadora, a través de la cual el usuario controla las operaciones que realiza el procesador.

Sistema Operativo

Termino que se utiliza para referirse al conjunto de programas interrelacionados, que se dedican a controlar las funciones básicas del sistema, las operaciones de bajo nivel y el manejo de archivos sin necesidad de que intervenga un operador.

Software Malicioso

Software que ha sido deliberadamente diseñado para producir un resultado defectuoso o dañoso para el usuario. Incluye tanto la categoría genérica de los virus informáticos, como la del llamado spyware.

TFTP

Protocolo trivial de transferencia de archivos. Utiliza el protocolo de datos de usuario (UDP) sin características de seguridad para transferir archivos.

Trabajo Remoto

Se refiere al trabajo que una persona realiza por fuera de su puesto de trabajo normal.

Trama

Los paquetes que contienen el encabezado y la información de cola que requiere el medio físico.

Tramas gigantes

Permiten transportar datos idénticos en menos tramas. Las tramas gigantes reducen el coste, necesitan un tiempo de procesamiento inferior y garantizan menos interrupciones.

Utilitarios del Sistema

Reconstruir índices, compactar y validar bases de datos, validar consistencia de datos, cambiar fecha de operación y del sistema, importar y exportar datos entre empresas, transferir productos, precios, existencias de almacén y acceso al generador de reportes.

Velocidad de puerto

Indica la velocidad del puerto. La velocidad de los puertos incluye:

Ethernet 10 Mbps
Fast Ethernet 100 Mbps
Gigabit Ethernet 1000 Mbps

BIBLIOGRAFÍA

- **Andrew Tanenbaum,** Redes de Computadores, Cuarta Edición 2004
- **Tyson Creer,** Así son las Intranets, Segunda Edición. 2002
- Building Cisco Multilayer Switched Networks; Cisco System, Cisco Press, 2000.
- Cisco CCNA Exam #640-607; Cisco System, Cisco Press, 2002.
- Implementing Cisco Quality of Service v 2.0; Cisco System, Cisco Press, 2003.
- **VLADIMIROV ANDREW A. (2005)**, Seguridad de redes Inalámbricas, EDICIONES AMAYA MULTIMEDIA, Madrid, España.
- **ANSI/IEEE STD 802.11, 1999** Edition. [1]"Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications"
- **Hills. "Large-Scale Wireless LAN Design"**. IEEE Communications Magazine, vol. 39, nº 11, noviembre 2001.

WEB BIBLIOGRAFÍA

- http://www.linuxparatodos.com/honeypot.htm
- http://www.linuxparatodos.com/ids.htm
- http://www.linuxparatodos.com/ips.htm
- http://lauca.usach.cl/~lsanchez/Vlan/
- http://www.eduangi.com/documentos/3_CCNA2.pdf
- http://www.avantel.net/~rcruz/Cap3qosrba.pdf
- http://www.lavioleta.net/Capitulo1.htm
- http://www.commlogik.com.ar/cisco.html
- http://informatica.uv.es/doctorado/SST/docto-2-qos.ppt#389,2,Sumario

- http://www.3com.es/news/reportajes/pdfs/switching_comunicaciones_world.pdf
- http://dmi.uib.es/~loren/docencia/webxtel/bibliografia/tutorial%20VLAN.pdf
- http://net21.ucdavis.edu/newvlan.htm
- http://www.itlp.edu.mx/publica/revistas/revista_isc/anteriores/jun99/vlan.html
- http://iie.fing.edu.uy/~rgaglian/Docs/VPLS.pdf
- http://www.emagister.com/frame.cfm?id_user=88930200502696748506748707045 55&id_centro=57953030052957564866666952674548&id_curso=65425040050167555457685550674555&url_frame=http://www.emagister.com/public/pdf/comunidad_emagister/01793120043168694849677065484567-config-ciscos.pdf
- http://www.it.iitb.ac.in/~it605/resources/Local/Docs/VLAN/VLANIntro.pdf
- http://www.isa.uniovi.es/docencia/redes/tema4.pdf
- http://www.mythdragon.com/QoS/documents/QoS%20routing%20for%20support%20MM%20apps.pdf
- http://www.alcatel.ch/com/en/appcontent/apl/A0506-Broadband_QoS-ES_tcm172-287901635.pdf
- http://www.adictosaltrabajo.com/linux/proxy.htm
- http://www.adictosaltrabajo.com/linux/proxyinverso.htm
- http://www.adictosaltrabajo.com/linux/firewall.htm
- http://www.adictosaltrabajo.com/linux/cortafuegos.htm
- http://www.monografias.com/proxy.htm
- http://www.monografias.com/firewall.htm
- http://www.cudi.edu.mx/primavera_2005/presentaciones/felipe_alvarez.pdf
- http://www.si.uji.es/bin/ponencies/ipp.pdf
- http://www.idg.es/comunicaciones/especial-avether160/Pag08.pdf
- http://www.iec.uia.mx/proy/titulacion/proy14/vpnprin.htm

ANEXO 1

1.- SELECCIÓN Y DELIMITACION DEL PROBLEMA

El constante avance tecnológico a nivel mundial hace que muchas instituciones y empresas investiguen y desarrollen algunas alternativas que permitan asegurar de mejor manera su información. Este tema discute o ayuda a la investigación de algunas medidas preactivas que pueden tomar los administradores de Redes de Telecomunicaciones para prevenir una violación a la seguridad, tal como la información de un equipo de respuestas a emergencias capaz de responder rápida y eficientemente ante problemas de seguridad.

A nivel de país el desarrollo e implementación de Servidores Trampa son escasos ya que implica una inversión en la utilización de nuevos servidores los mismos que serian utilizados solamente para la detección de posibles intrusiones, por lo que son temas solamente de investigación mediante Maquinas Virtuales y que por su alto nivel de seguridades en un futuro no muy lejano se podrían implementar.

En la provincia de Cotopaxi al contar con muchas empresas y plantaciones de flores una investigación de este tipo realizada en nuestra universidad seria un aporte significativo ya que estaríamos brindando a los dueños de todas las empresas e instituciones una alternativa de seguridades, a nivel físico y al ser realizado mediante Maquinas Virtuales se optimizaría el recurso físico y económico.

A lo expuesto anteriormente y ante la necesidad existente de mejorar la funcionalidad de las redes de comunicaciones asegurando la información y lo más importante en estos temas es que como conclusión a un tema de este tipo seria la Investigación de cómo los Hackers y Crackers realizan sus ataques a las empresas o instituciones, este tema: **"DESARROLLO DE PRUEBAS DE UN HONEYPOTS (SERVIDORES TRAMPA) PARA DETECCIÓN DE INTRUSOS**, podría ser potenciado de mejor manera con el estudio posterior o como tema de investigación en el área de Informática Forense.

2.- PLANTEAMIENTO DEL PROBLEMA

Las propiedades de gran valor necesitan ser protegidas de robo o destrucción potencial. Algunos hogares están equipados con sistemas de alarmas que pueden detectar ladrones, notificar a las autoridades cuando ocurre una entrada ilegal y hasta advertir a los dueños cuando sus hogares están bajo fuego. Tales mediadas son necesarias para asegurar la integridad de los hogares y la seguridad de sus dueños.

El mismo aseguramiento de la integridad y seguridad debería ser aplicado a los sistemas de computación y datos. La Internet ha facilitado el flujo de información, desde personal hasta financiera. Al mismo tiempo, también ha promovido muchos peligros. Los usuarios maliciosos y crackers buscan objetivos vulnerables tales como sistemas no actualizados, sistemas infectados con troyanos redes ejecutando servicios inseguros, servidores con

puertos abiertos que pueden ser potenciales puertas de acceso a la información.

Las alarmas son necesarias para notificar a los administradores y a los miembros del equipo de seguridad que ha ocurrido una entrada ilegal para que así estos puedan responder en tiempo real a la amenaza. Se han diseñado Servidores Trampa denominado Honeypots por su nombre en Ingles como medida para desviar la atención de los crackers del servidor que si contiene la información que se trata de precautelar.

3.- ENUNCIADO DEL PROBLEMA

Como producto de la investigación realizada en algunas empresas y sitios donde hemos podido prestar nuestros servicios profesionales hemos podido detectar muchos problemas al no poder contar con algunas alternativas de aseguramiento de la información, siendo este un gran inconveniente ya que toda la información está sujeta a eliminaciones o alteraciones de la misma.

A través del levantamiento de un diagnostico llevado a cabo por el grupo investigador se la podido detectar que el problema es el siguiente.

¿La nesecidad de desarrollar las pruebas de un (HONEYPOTS) Servidores Trampa permitirá garantizar la integridad de la información de una red de comunicación?

4. – JUTIFICACION

Al momento de realizar un análisis para un futuro desarrollo de un Servidor Trampa ampliamos de igual manera algunas alternativas de temas de investigación, ya que producto de está investigación hemos podido ver que temas de este tipo se justifican con un posterior desarrollo de una Informática Forense, la misma que permite determinar con precisión el ataque que fue victima las empresas que adaptaron como alternativa a los (Honeypots) Servidores Trampa.

El desarrollo de un (Honeypots), Servidor Trampa resulta muy importante tanto en el área de investigación como en la tecnológica, ya que al tratarse de nuevas alternativas de seguridades en las redes estaríamos garantizando de alguna manera la integridad de la información de las empresas o instituciones que pueden mirar a un Honeypots como una alternativa valida al momento de decidir la seguridad de su infraestructura.

La necesidad e importancia de temas de este tipo es de ampliar el área de investigación de la Ingeniería en Informática y Sistemas Computacionales y la otra es brindar a la sociedad cotopaxense una alternativa en lo que tiene que ver con Seguridades de la Información.

Es por estas razones que hemos creído conveniente desarrollar un Honeypots como alternativa valida de proporcionar seguridades a las infraestructuras de red.

5. – OBJETIVOS

5.1 OBJETIVO GENERAL

- Desarrollar las pruebas de un Honeypots (Servidor Trampa) para garantizar la integridad de la información en una red de comunicación.

5.2 OBJETIVOS ESPECÍFICOS

- Realizar un análisis de las diferentes arquitecturas de servidores.
- Diseñar la alternativa de seguridades mediante servidores.
- Etiquetar transmisiones sospechosas, que son recibidas en el Servidor Trampa, para prevenir desastres.
- Plantear alternativas de seguridades dentro del protocolo TCP/IP, bajo scaners, husmeadores y otras herramientas de auditoria y prevención de intrusos.

6. – MARCO TEORICO

El presente trabajo investigación estará constituido bajo los siguientes lineamientos:

6.1 ANTECEDENTES

Nuestra investigación se lo realizara en empresas amigas, así como en la Universidad Técnica de Cotopaxi, y concretamente en el área de Ingeniería en Sistemas los mismos que van a ser tomados en cuenta los docentes, y alumnos de los últimos ciclos de la Especialidad de Ingeniería en Sistemas que pueden tener conocimiento de algunas de estas nuevas tecnologías.

6.2 BASES TEORICAS

Considerando que nuestro objeto de estudió es un análisis, fundamentaremos científicamente nuestra investigación citando conceptos y categorías de varios autores.

Según la dirección linuxparatodos.com/redes/tutoriales/honeypot.html; "El papel de la tecnología del sistema de detección de intrusos basado en señuelos o "honeypots" está evolucionando. Los honeypots, que alguna vez fueron utilizados principalmente por los investigadores como una forma de atraer a los hackers a un sistema de redes para estudiar sus movimientos y comportamiento, están adquiriendo una importancia cada vez mayor en la seguridad empresarial. En efecto, al brindar detección temprana de actividad no autorizada en las redes, los honeypots son ahora más útiles que nunca para los profesionales de seguridad de TI. Este artículo analiza el funcionamiento de los honeypots y su tecnología, que se está convirtiendo en el componente clave del sistema de capas de protección contra intrusos.

Los Honeypots son una emocionante tecnología nueva, con un enorme potencial para la comunidad informática. Los primeros conceptos fueron introducidos por primera vez por varios iconos en la seguridad informática, especialmente por Cliff Stoll en el libro "The Cuckoo's Egg" y el trabajo de Bill Cheswick "An Evening with Berferd". Desde entonces, los honeypots han estado en una continua evolución desarrollándose en una poderosa herramienta de seguridad hoy en día. El propósito del presente trabajo es el de explicar exactamente que son los honeypots, sus ventajas y desventajas, y su importancia en la seguridad.

Los Honeypots (Potes de miel) "Consisten en activar un servidor y llenarlo de archivos tentadores, hacer que sea difícil, pero no imposible penetrarlo y sentarse a esperar que aparezcan los intrusos. Los honeynets (conjuntos de honeypots) dan a los crackers un gran espacio para recorrer. Presentan obstáculos que poseen el nivel de complejidad suficiente para atraerlos, pero sin irse al extremo para no desalentarlos. Ellos juegan con los archivos y conversan animadamente entre ellos sobre todo los fascinantes programas que encuentran, mientras el personal de seguridad observa con deleite cada movimiento que hacen. Francamente, siento una combinación de sentimientos con respecto a espiar a la gente, aunque no sean buenas personas".

Según la dirección: http://www.monografias.com/manuales/inform/honeytramp.html,"Manifiesta que el concepto de Honeypots no fue extraído o inventado de la nada, sino que es fruto de la realización de varios estudios en el campo de la seguridad de redes de ordenadores

[Sch99][Hon01][Mcm01][Kue02][Ran02][VP02][Lev03].

Definiremos Honeypots (tarro de miel textualmente) como "un recurso de red destinado a ser atacado o comprometido. De esta forma, un Honeypots será examinado, atacado y probablemente comprometido por cualquier atacante. Los Honeypots no tienen en ningún caso la finalidad de resolver o arreglar fallos de seguridad en nuestra red. Son los encargados de proporcionarnos información valiosa sobre los posibles atacantes en potencia a nuestra red antes de que comprometan sistemas reales [Spit02]".

Esta nueva aproximación a la seguridad de redes de ordenadores rompe muchos tabúes clásicos que se daban como axiomas en la seguridad informática "clásica":

• Por un lado, este nuevo elemento no sirve para eliminar o corregir fallos de seguridad existentes en nuestra red. Si nuestra red es vulnerable, añadir un Honeypots no solventará este fallo.

• Por otro lado, en lugar de evitar a cualquier precio que un atacante fije su interés en nuestra red, le invitamos (para ser exactos deberíamos decir le permitimos) a que entre y ataque nuestra red.

Este interés en dejar una puerta abierta hacia Internet puede considerarse temeraria o incluso suicida. Si ya existen cientos de miles de ataques a sistemas "seguros" ¿porqué dejar un pote de miel en medio del camino del "oso"? ¿Por qué incitar a que ataquen nuestro sistema cuando nuestro objetivo es conseguir exactamente lo

contrario?.

Por muy eficientes que seamos en nuestro trabajo como administradores de red, es imposible mantener todos nuestros sistemas al día (up to date). Cada día se descubren al menos una docena de nuevos fallos (bugs) en el software existente [WWW21] (sistemas operativos, servidores de aplicaciones, servidores WWW).

Según la dirección http://es.tldp.org/Tutoriales/doc-servir-web-escuela/doc-servir-web-escuela-html/redes.html, define **REDES** como: "Un conjunto de ordenadores capaces de comunicarse entre sí, bien directamente, o a través de otros. Como en toda comunicación, para que ésta sea posible, necesitamos un idioma que sea comprendido por todos los integrantes, en este caso, los ordenadores de la red. En este contexto el idioma es el protocolo de comunicación".

De acuerdo a esta dirección, **REDES** es un conjunto de ordenadores que mantiene una estricta relación entre si, que permitirá mantener una comunicación eficaz entre usuarios; por lo tanto es de gran utilidad realizar un análisis del control y flujo de la red.

En cambio la dirección, http://moncayo.unizar.es/ccuz/proced.nsf/0/5f94OpenDocument, dice que **REDES** es: "Una serie de ordenadores y otros dispositivos conectados por cables entre sí. Esta conexión les permite comunicarse entre ellos, compartir información y recursos".

De acuerdo a esta dirección, **REDES** es un sistema de comunicación entre computadoras, que permite compartir información y recursos; razón por la cual este

análisis del control y flujo de la red ayudara a resolver los problemas por los que atraviesa la red de la Universidad Técnica de Cotopaxi.

Para la dirección http://w3.mor.itesm.mx/~lssalced/remota.html, define **REDES**: "Un conjunto de computadoras que usan el mismo PROTOCOLO para intercambiar información entre ellas".

De acuerdo con esta dirección **REDES** es un sistema de comunicaciones entre computadoras utilizando un mismo protocolo; por lo que será de gran importancia realizar este análisis del flujo de la red ayudando de alguna manera resolver los problemas por los que atraviesa la red en la Institución.

6.3 DEFINICIÓN DE TERMINOS BÁSICOS

ANCHO DE BANDA.- En conexiones a Internet el ancho de banda es la cantidad de información o de datos que se puede enviar a través de una conexión de red en un período de tiempo dado. El ancho de banda se indica generalmente en bites por segundo (BPS), kilobytes por segundo (kbps), o megabytes por segundo (mps). En general, una conexión con ancho de banda alto es aquella que puede llevar la suficiente información como para sostener la sucesión de imágenes en una presentación de video.

CRACKER.- Es alguien que viola la seguridad de un sistema informático, el cracker realiza la intrusión con fines de beneficio personal o para hacer daño.

HACKER.- Experto en redes y seguridad que accede a sistemas a los que no tiene autorización sin ánimo de causar daño, generalmente para aprender más.

HONEYNETS.- (Conjuntos de honeypots) dan a los crackers un gran espacio para recorrer. Presentan obstáculos que poseen el nivel de complejidad suficiente para atraerlos, pero sin irse al extremo para no desalentarlos. Ellos juegan con los archivos y conversan animadamente entre ellos sobre todo los fascinantes programas que encuentran, mientras el personal de seguridad observa con deleite cada movimiento que hacen.

HONEYPOTS.- Los Honeypots (Potes de miel) Consisten en activar un servidor y llenarlo de archivos tentadores, hacer que sea difícil, pero no imposible penetrarlo y sentarse a esperar que aparezcan los intrusos.

HOST.- Computadora con funciones centralizadas que hace disponibles programas a otras computadoras.

HUB.- El ancho de banda es compartido por todos los puertos mediante una múltiplexación (solo una estación puede transmitir de un puerto a otro en cada instante).

INTERNET.- Conjunto de millones de computadores conectadas entre si a nivel mundial.

PROTOCOLO.- Es un estándar que define el método de comunicación entre

computadoras. Esto es el lenguaje y las reglas gramaticales que las computadoras acuerdan usar para entenderse. El protocolo para Internet es conocido como TCP/IP (Transmisición Control Protocol/Internet Protocol).

REDES.- Las redes en general, consisten en "compartir recursos", y uno de sus objetivos es hacer que todos los programas, datos y equipo estén disponibles para cualquiera de la red que así lo solicite, sin importar la localización física del recurso y del usuario. En otras palabras, el hecho de que el usuario se encuentre a 1000 Km. de distancia de los datos, no debe evitar que este los pueda utilizar como si fueran originados localmente.

RED DE ÁREA LOCAL (Local Área Network) LAN.- Es un sistema de comunicación entre computadoras, que permite compartir información y recursos, con la característica de que la distancia entre las computadoras debe ser pequeña.

RED DE ÁREA METROPOLITANA (Metropolitan Área Network) MAN.- Es una versión de mayor tamaño de la red local. Puede ser pública o privada. Una MAN puede soportar tanto voz como datos. Una MAN tiene uno o dos cables y no tiene elementos de intercambio de paquetes o conmutadores, lo cual simplifica bastante el diseño. La razón principal para distinguirla de otro tipo de redes, es que para las MAN's se ha adoptado un estándar llamado DQDB (Distributed Queue Dual Bus) o IEEE 802.6. Utiliza medios de difusión al igual que las Redes de Área Local.

RED DE DATOS.- Conjunto de dispositivos conectados entre si con el fin de compartir datos.

REPETIDORES.- Son equipos que actúan a nivel físico. Prolongan la longitud de la red uniendo dos segmentos y amplificando la señal, pero junto con ella amplifican también el ruido. La red sigue siendo una sola, con lo cual, siguen siendo válidas las limitaciones en cuanto al número de estaciones que pueden compartir el medio.

ROUTERS (ENCAMINADORES).- Son equipos de interconexión de redes que actúan a nivel de los protocolos de red. Permite utilizar varios sistemas de interconexión mejorando el rendimiento de la transmisión entre redes. Su funcionamiento es más lento que los bridges pero su capacidad es mayor. Permiten, incluso, enlazar dos redes basadas en un protocolo, por medio de otra que utilice un protocolo diferente.

SERVIDOR.- Se denomina así al ordenador que se encarga de suministrar lo necesario a una red, dependiendo de cual sea la finalidad de ésta.

SISTEMA OPERATIVO.- Es aquel programa (Software) que es capaz de acceder al Hardware (dispositivos físicos) de un ordenador, y ofrece al usuario un lenguaje sencillo para realizar esta tarea. Así pues el Sistema Operativo es una capa que encontramos entre el usuario y el hardware, de forma que el usuario trabaja con comodidad y sencillez y es el Sistema Operativo el que realiza el trabajo duro de forma más o menos transparente.

SISTEMA OPERATIVO LINUX.- Es la denominación de un sistema operativo y el nombre de un núcleo. Es uno de los paradigmas del desarrollo de software libre (y de código abierto), donde el código fuente está disponible públicamente y cualquier persona, con los conocimientos informáticos adecuados, puede libremente estudiarlo, usarlo, modificarlo y redistribuirlo. El software que suelen incluir consta de una enorme variedad de aplicaciones, como: entornos gráficos, suites ofimáticas, servidores Web, servidores de correo, servidores FTP, etc.

SPAM.- Es el nombre con que las personas llaman a los correos electrónicos no deseados recibidos en la Internet. La idea es que si los usuarios de Internet simplemente fueran inundados por el spam, nadie podría distinguir el spam de los correos electrónicos normales.

SWITCH.- Es la tecnología más sencilla y económica para mejorar el desempeño de una red muy ocupada.

TCP-IP.- Transmisión Control Protocol-Internet Protocol. Protocolo en el que se basa Internet y que en realidad consiste en dos. El TCP, especializado en fragmentar y recomponer paquetes, e IP para diseccionarlos hasta su destino.

WAN (Wide Área Network).- Redes de Amplia Cobertura, son redes que cubren una amplia región geográfica, a menudo un país o un continente. Este tipo de redes contiene máquinas que ejecutan programas de usuario llamadas hosts o sistemas finales (end system). Los sistemas finales están conectados a una subred de

comunicaciones. La función de la subred es transportar los mensajes de un host a otro.

7. – HIPÓTESIS

El Desarrollo de pruebas de un (Honeypots) Servidor Trampa permitirá garantizar la integridad de la información en una red de comunicación.

8. – VARIABLES E INDICADORES

8.1 VARIABLE INDEPENDIENTE

Desarrollo de pruebas de un (Honeypots) Servidor Trampa.

INDICADORES

- Detectar posibles intrusos.
- Evitar abusos al sistema.
- Perdida de recursos económicos.

8.2 VARIABLE DEPENDIENTE

Permitirá garantizar la integridad de la información en una red de comunicación.

INDICADORES

- Optimizar el servicio de los servidores.
- Rapidez en la prestación de servicios.
- Establecer un control para el aseguramiento de la información.

9. – ESQUEMA DE CONTENIDOS

- Portada.
- Pagina de Responsabilidad de Autoría.
- Certificación del Director de Tesis.
- Certificación de la Institución objeto de estudio.
- Agradecimiento.
- Dedicatoria.
- Índice General.
- Índice de Cuadros.
- Índice de Tablas.
- Resumen.
- Abstrac.
- Certificación del Abstrac.
- Introducción.

Esta tesis comprende de tres capítulos los mismos que fundamentan lo siguiente:

CAPITULO I

FUNDAMENTACIÓN TEÓRICA DE LAS SEGURIDADES BASADAS EN SERVIDORES

1.1 (HONEYPOT Y HONEYNET) SERVIDORES TRAMPA

1.1.1 Introducción y Sinopsis

1.1.2 Características de los Honeypot

1.1.3 Características de los Honeynet

1.1.4 Sinopsis tecnológica y configuración

1.1.5 Requisitos del Sistema

1.1.6 Análisis Informático Forense

1.2 SISTEMAS DE DETECCION Y PREVENCION DE INTRUSOS

1.2.1 Definiciones de Intrusos e Intrusiones

1.2.2 Tipos de de Intrusos e Intrusiones

1.2.3 Sistemas Operativos soportados

1.2.3.1 Linux

1.2.3.2 Windows

1.2.3.3 Solaris

1.3. Sistema de Seguridades

1.3.1. Definición de seguridad

1.3.2. Tipos de Seguridades en Redes de telecomunicaciones a nivel de Servidores

CAPITULO II

TRABAJO DE CAMPO

ELEMENTOS NECESARIOS PARA LAS CONFIGURACIONES DE LOS (HONEYPOTS) SERVIDORES TRAMPA

2.1 Parámetros necesarios a ser considerados en las configuraciones de los Honeypots.

2.2 Estándares de calidad de servicio y rendimiento a seguir para la instalación y configuraciones de los Servidores Honeypots.

2.3 Logros e Insuficiencias encontradas en la manera de implementación en equipos físicos.

2.4 Análisis de los resultados obtenidos de las fuentes consultadas, a nivel de administración de departamento de Sistemas Área de Seguridad, docentes y estudiantes de la especialidad de Sistemas.

2.5 Verificación de Hipótesis.

2.6 Conclusiones.

2.7 Recomendaciones.

CAPITULO III

DESARROLLO DE PRUEBAS DE UN (HONEYPOTS) SERVIDOR TRAMPA

Sistema operativo Linux

3.1. Factibilidad.

3.1.1. Factibilidad Técnica.

3.1.2. Factibilidad Económica.

3.1.3. Factibilidad Operacional.

3.2. Diseño Físico de las redes planteado, para garantizar seguridades con un Servidor Trampa.

3.2.1. Acceso ilimitado a Internet.

3.2.2. Acceso limitado a Internet.

3.3. Implementación de seguridades Lógicas mediante Honeypots.

3.3.1. Local.

3.3.2. Externa.

3.5. Emulación de Servicios.

3.6. Emulación de Puertos Abiertos.

3.7. Principios Básicos de la Informática Forense.

10. – POBLACIÓN Y MUESTRA

10.1 POBLACIÓN

La investigación propuesta se realizara con la colaboración de algunos profesionales que se desempeñen en el área de Ingeniería en Sistemas, además de que esperamos contar con los estudiantes de los últimos ciclos de la Especialidad de Ingeniería en Sistemas de la Universidad Técnica de Cotopaxi de la ciudad de Latacunga; las encuestas estarán enfocadas a los administradores y a los usuarios de los laboratorios, mientras tanto las entrevistas estarán enfocadas a los administradores de los laboratorios únicamente.

CUADRO Nº 10.1

POBLACION INVOLUCRADA

INVOLUCRADOS	CANTIDAD
Administradores de Redes	10
Estudiantes de los Últimos Ciclos de Ingeniería en Sistemas.	350
Docentes de Sistemas	15
Total	375

FUENTE: Encuesta

REALIZADO POR: Los investigadores

10.2 MUESTRA

Para obtener una muestra representativa de la población investigada se opto por la muestra no probabilística para los administradores de las áreas de redes, docentes y probabilística para los estudiantes de los últimos ciclos de la especialidad de Ingeniería en Sistemas., de la siguiente manera.

Con relación a los administradores de la red se considero conveniente seleccionar un universo del (100 %).

En el caso de los docentes se aplico a un 100 % para obtener información sobre las dificultades en el rendimiento de las conexiones par la búsqueda de información y la necesidad de elaborar una propuesta que ayude a obtener máximo rendimiento en el sistema.

En relación a los estudiantes de la especialidad de Ingeniería en Sistemas, se tomo una muestra probabilística estratificada para llegar a establecer el numero de la muestra.

FORMULA:

$$n = \frac{NO^2 Z^2}{(N-1)E^2 + 0^2 Z^2}$$

DONDE:

n = Tamaño de la muestra

N = numero de población

O = 0,5 de varianza

Z = 1,96 Nivel de Confianza

E = 0,06 Error Máximo Admisible

Reemplazando los valores en la formula tenemos:

$$\mathbf{n} = \frac{350 * 0.5^2 * 1.96^2}{(350-1)0,06^2+0,5^2*1,96^2}$$

$$n = \frac{350 * 0{,}25 * 3{,}8416}{(349)\ 0{,}0036 + 0{,}25 * 3{,}84\ 16}$$

$$n = \frac{336.14}{1.2564 + 0{,}9604}$$

$$n = \frac{336.14}{2.2168}$$

n= 151.63

CUADRO 10.2

MUESTRA DE LA POBLACIÓN INVOLUCRADA

INVOLUCRADOS	POBLACIÓN	MUESTRA
Administradores de Redes	10	10
Estudiantes de los Últimos Ciclos de Ingeniería en Sistemas	350	152
Docentes de Sistemas	15	15
Total	375	277

FUENTE: Encuesta

REALIZADO POR: Los investigadores

11. – PROCEDIMIENTO METODOLOGICO

11.1 TIPO DE INVESTIGACIÓN

Para la realización del estudio de este trabajo se utilizara la **Investigación Descriptiva** que nos permitirá tener un contacto con la realidad y las fuentes directas que guarden relación con el flujo de la información para el mejoramiento de las seguridades en donde se puedan aplicar este tipo de investigación; este análisis nos permitirá desarrollar y presentar nuevos puntos de vista, que nos van a servir como referencia para interpretar los diferentes procesos que se encuentren en la elaboración del proyecto, y para un mejor soporte nos apoyaremos en la **Investigación Bibliográfica**.

11.2 MÉTODOS

Para el presente trabajo de investigación se utilizaran los siguientes métodos:

Método Explicativo e Hipotético Inductivo.- Para alcanzar los objetivos propuestos y a la vez comprobar la hipótesis planteada.

Método Dialéctico.- Permitirá explicar las casualidades y procesos lógicos del problema y de ésta manera conocer su rol significativo.

Y para una correcta formulación de la investigación se aplicarán:

Métodos Empírico.- Que llevara a una correcta formulación de las encuestas,

entrevistas y análisis documental con los cuales se describirán las propiedades permitiendo establecer criterios que nos lleven a un entendimiento claro de las variables y a formular las vías de evolución que faciliten mejorar los procesos para dotar de mayor agilidad al sistema.

11.3 TÉCNICA

La técnica es indispensable en el proceso de la investigación, ya que integra la estructura por medio de la cual se organiza la investigación; se utilizara las siguientes técnicas: Encuestas, entrevistas, observación, bibliográfica.

ENTREVISTAS.- Mediante esta técnica se obtendrá datos que consisten en un diálogo entre dos personas: El entrevistador "investigador" y el entrevistado; se realizara con el fin de obtener información importante de parte del entrevistado; se aplicara a la Administración General, Administración Financiera, Dep. Justicia, Policía y Vigilancia, Sección Educación y Cultura y Otros Servicios Comunales.

ENCUESTA.- Es una técnica destinada a obtener datos de varias personas cuyas opiniones impersonales interesan al grupo investigativo. Para ello, se utilizara un listado de preguntas escritas que se entregaran a los trabajadores, contratados y contribuyentes de la Municipalidad, a fin de que las contesten igualmente por escrito.

OBSERVACIÓN.- Se utilizara la observación para deducir las falencias que posee la municipalidad y reunir información que se empleara para interpretar aciertos y describir hechos.

TECNICA BIBLIOGRÁFICA.- Esta técnica se empleara como apoyo en la recolección de información y anotaciones de datos necesarios para sustentar el trabajo investigativo.

11.4 INSTRUMENTOS

Los Instrumentos que se aplicaran para el trabajo de investigación son los siguientes:

GUIA DE ENTREVISTA.-Se realizara en forma individual, por medio de esta se obtendrá información sobre el objeto de investigación, se planteara soluciones.

FORMULARIO DE PREGUNTAS.- Se empleara para uniformar la observación, establecer total atención a los aspectos esenciales de la investigación y precisar la información requerida. Estará constituida por 10 preguntas las cuales serán cortas, se empleara términos claros y precisos, y se utilizaran preguntas cerradas que permitan solo una opción para contestar ya que facilitara el procesamiento de la información; además se dará instrucciones para el manejo de las encuestas.

GUIA DE OBSERVACIÓN.- Estará diseñado de acuerdo a nuestro trabajo de investigación el mismo que nos ayudara a reunir información precisa relacionada con nuestro tema de investigación.

FICHAS TEMATICAS.- Que recolectaran información bibliográfica sobre temas concretos que se refieren al objeto de investigación propuesto.

FICHAS BIBLIOGRAFICAS.- Proporcionando dato específicos sobre libros, revistas, etc.

12. – DISEÑO ESTADÍSTICO

En esta investigación se tomara como base a los diferentes sectores como administradores de redes, estudiantes y docentes de la especialidad de Ingeniería en Sistemas de la Universidad Técnica de Cotopaxi.

Para el procesamiento de la información se utilizara la **Estadística Descriptiva** por cada variable, para la tabulación de las respuestas enmarcados en los cuestionarios, organizados en una matriz de datos, para obtener cuadros de distribución de frecuencias en histogramas

13. – RECURSOS

13.1 HUMANOS

Los responsables de este trabajo investigativo son:

Director:

Ing. Patricio Navas

Postulantes:

Molina Castellano Mayra Lili

Tapia Toctaguano Alexandra Verónica

13.2 MATERIALES

- Hojas de papel INEN A4
- Carpetas
- Esferos
- Cuadernos
- Portaminas
- Copias de documentos

13.3 TECNOLÓGICOS

- Uso de maquina
- Flash Memory 1GB
- CD's
- Internet.
- Impresora.
- Cartuchos de tinta
- Scanner.

14. - PRESUPUESTO

El presupuesto para la realización de este trabajo de investigación se presenta en el siguiente cuadro.

CUADRO Nº 14.1

COSTOS DIRECTOS

DETALLE	CANTIDAD	VALOR/UNIT	TOTAL
Hojas de papel INEN A4	1200	0.02	24.00
Carpetas	5	0.15	0.75
Esferos	9	0.25	2.25
Cuadernos	2	3.00	6.00
Portaminas	3	1.50	4.50
Copias de documentos	600	0.02	12.00
Uso de maquina	500	0.08	400.00
Flash Memory	1	20.00	20.00
CD's	1	1.30	3.90
Internet	250	0.70	175.00
Impresiones	1200	0.15	180.00
Cartuchos de tinta	4	25	100.00
Escáner.	20	0.25	5.00

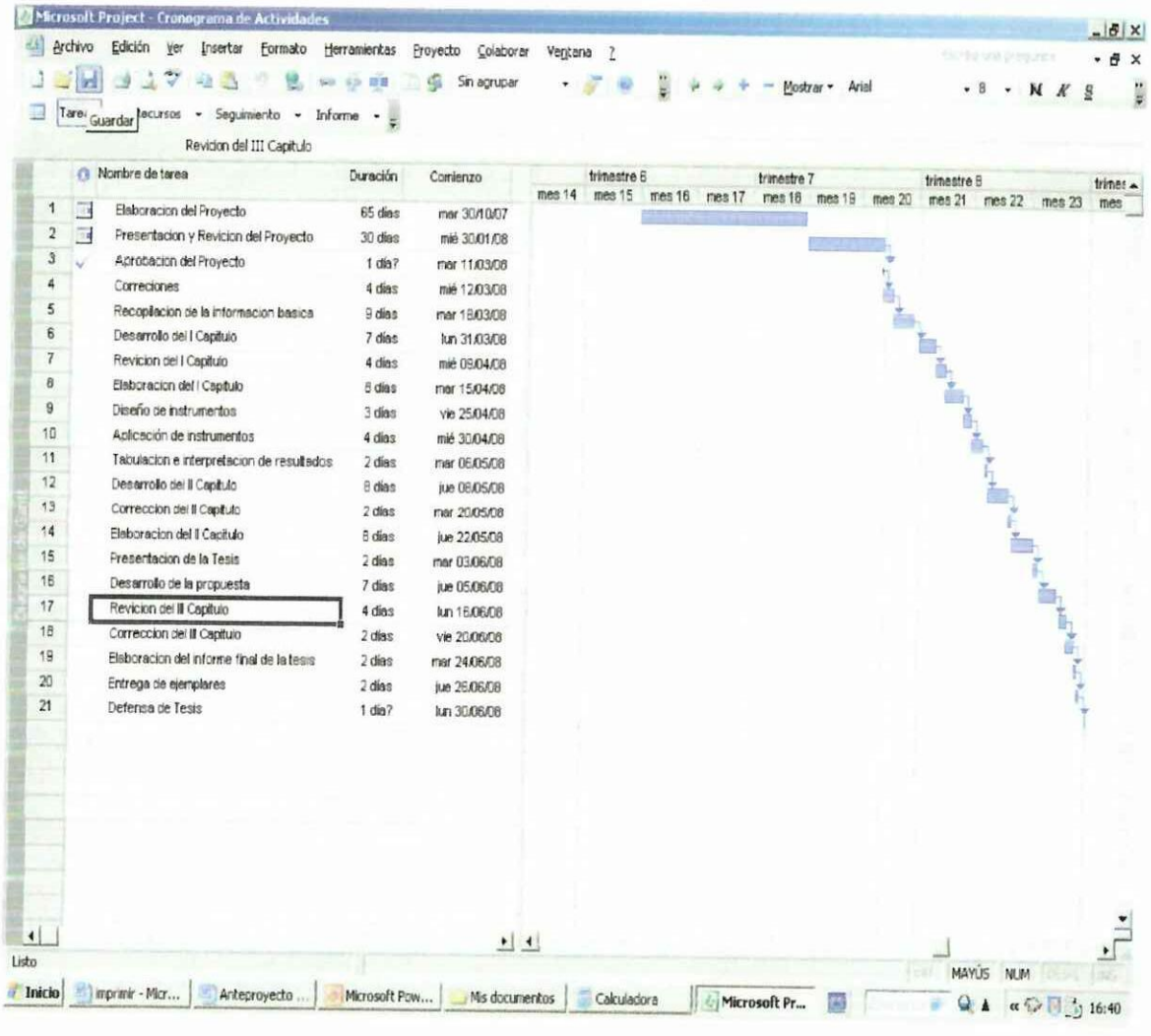
COSTOS INDIRECTOS

NOMINA	TOTAL
Viáticos	300.00
Trasporte	200.00
Comidas	150.00

SUB-TOTAL 1583.40

(+) 10% IMPREVISTOS	100.00
COSTO TOTAL DEL PROYECTO	1683.40

15. – CRONOGRAMA



16. – BIBLIOGRAFÍA

16.1 BÁSICA

- http://www.monografias.com/trabajos10/teut/teut.shtml#ob
- http://www.ual.mx/servicios/ccomputo.html
- http://apuntes.rincondelvago.com/variables-en-la-investigacion.html
- http://www.monografias.com/trabajos11/metcien/metcien.shtml#METO
- http://www.monografias.com/trabajos12/muestam/muestam.shtml#INTRO
- http://www.monografias.com/trabajos11/metods/metods.shtml#LOGICO

16.2 CONSULTADA

DYSON, Peter (1999); Diccionario de Redes; Editorial McGraw-Hffl; Bogotá.

RODRÍGUEZ, Jorge (1999); Introducción a las Redes de Área Local; Editorial McGraw-Hill; México.

TENEMBAUM ANDREW S. (1999); Sistemas Operativos Distribuidos; Editorial Prentice Hall; México.

16.3 CITADA

- linuxparatodos.com/redes/tutoriales/honeypot.html
- http://www.monografias.com/manuales/inform/honeytramp.html
- http://es.tldp.org/Tutoriales/doc-servir-web-escuela/doc-*servir*-web-escuela-html/redes.html

- http://w3.mor.itesm.mx/~lssalced/remota.html
- http://moncayo.unizar.es/ccuz/proced.nsf/0/5f94OpenDocument

16.4 VIRTUAL

- http://infase.es/FORMACION/INTERNET/tcpip.html
- http://www.abcdatos.com/
- http://usuarios.lycos.es/redes
- http://www.todo-linux.com/modules.php?name=News&file=article&sid=4539
- http://radaman.blogspot.com/2006/10/qu-es-un-honeypot.html
- http://www.rzw.com.ar/seguridad-informatica-2237.html
- http://www.jessland.net/JISK/Honeypots.php
- http://his.sourceforge.net/honeynet/papers/vmware/
- http://www.webhostinghispano.com/forums/showthread.php?t=2702
- http://inestable.org/files/Honeypots.pdf
- http://es.wikipedia.org/wiki/Honeypotc
- http://www.monografias.com/trabajos/solinux/solinux.shtml
- http://el-directorio.org/Seguridad/Honeypots
- http://perso.wanadoo.es/aemulus/linux/
- http://www.monografias.com/Computacion/Redes/
- http://www.monografias.com/trabajos/introredes/introredes.shtml