Honeypot: Ventajas y Desventajas como Mecanismo para la Prevención de Intrusos Informáticos

Arenas Eduard, López Daniel
eduard.arenas@gmail.com, lcdaniel04@gmail.com
Universidad Piloto de Colombia

Abstract— Through the development and presentation of this document seeks to present the concepts of Honeypots, definition, classification, advantages and disadvantages, as well as their location and use the IDS. In addition, the usefulness and legal implications of implementation. Also, will address the issue of the impact they have had and the different fields where you can apply today. Finally, an analysis and recommendations for best benefit and implement a Honeypot in our organizations.

Resumen— Mediante la presentación y desarrollo de este documento se busca dar a conocer los conceptos sobre Honeypots, definición, clasificación, ventajas y desventajas, así como la ubicación de los mismos y la utilización con los IDS. Además, la utilidad y las implicaciones legales que conlleva la implementación. También, se abordará el tema sobre el impacto que han tenido y los diferentes campos en donde se pueden aplicar hoy en día. Y por último se realiza un análisis y recomendaciones para así sacar mayor provecho de implementar un Honeypot en nuestras organizaciones.

Índice de Términos— Firewall, Hacker, Hacking, HoneyNet Honeypot, IDS, Intrusos, IPv4, IPv6, Protección.

I. INTRODUCCIÓN

En la actualidad no existe la seguridad total en ningún sistema, así se trate de Organizaciones con los recursos tecnológicos más sofisticados como lo son los Firewall, IDS (Sistema de Detección de Intrusos), ya que estos mecanismos de detección y prevención no son suficiente para contrarrestar un ataque informático malintencionado.

Para las organizaciones, el activo más importante es la información, la cual es de vital importancia para el desarrollo de sus actividades diarias, por tal razón se debe obtener una infraestructura de seguridad de red acorde a los objetivos del negocio como base para un diseño de una red con una seguridad optima mediante mecanismos de seguridad que nos ayude a prevenir, diagnosticar y desviar un ataque o intrusión a las redes de las organizaciones.

Sí observamos un poco las estadísticas, en la actualidad existen aproximadamente 189 millones de cibernautas [1] a nivel de América del Sur, y un porcentaje de penetración del 48.2% en la misma región; sin embargo, un gran número de usuarios, administradores o proveedores que se encuentran dentro de una red no tienen un conocimiento claro de las debilidades, vulnerabilidades o huecos de seguridad a los que están expuestos sus activos de información ni del crecimiento exponencial que ha tenido la actividad de los Hackers en los últimos años en la región.

Esta es una de las razones por la que existen diferentes métodos y sistema para evitar ataques, uno de estos es el Honeypot cuya intención es la de atraer a atacantes, simulando ser sistemas de producción vulnerables o débiles a los ataques informáticos, este método cuando se combina con un sistema de detección de intrusos, IDS nos permite diagnosticar mediante las diferentes firmas y reglas que se configuran en el dispositivo inicialmente, con una mayor exactitud y rapidez como el atacante pudo ingresar de forma ilegal a la red de las organizaciones.

II. ANTECEDENTES

Para poder realizar una profundización sobre las ventajas y desventajas de los Honeypots, es necesario realizar una contextualización de este componente, así como mencionar en donde pueden

ser ubicados.

III. QUE ES UN HONEYPOT

El Honeypot, es un recurso de red destinado a ser atacado o comprometido [2] con la finalidad de obtener información acerca de los métodos que utiliza un atacante para ingresar.

Es una trampa que se utiliza para identificar, evitar y, en cierta medida, neutralizar los intentos de secuestrar los sistemas de información y redes.

Ejemplo. Se puede engañar al atacante haciéndolo pensar que se encuentra frente a una red poco segura y con huecos de seguridad que él pueda explotar.

Un Honeypot, es generalmente utilizado como sistema de vigilancia, así como un mecanismo de alerta temprana.

Los Honeypots provienen de una expresión inglesa que podría traducirse como -tarros de miel- o señuelos diseñados para proteger los sistemas informáticos de Hackers, emisores de correo basura y ataques automatizados, como los virus, troyanos y gusanos. En esencia, se trata de un software o conjunto de computadores que se exponen deliberadamente para ser atacados como anzuelos en las redes de las organizaciones.

La táctica empleada por un administrador de un Honeypot, es la de simular un ambiente tentador de producción el cual debe tener un atractivo muy importante que capte la atención del atacante, por ejemplo: un sistema que contenga un servidor de base de datos o de Front, ya que estos son los sistemas que son más propensos a ser atacados y que también brinde un reto al atacante al momento de ejecutar alguna técnica o metodología de intrusión. Así se consigue un doble objetivo; por una parte se desvía la atención de los atacantes de la red que contiene la información valiosa y por otra, se construyen perfiles que permitan analizar las estrategias que aquellos siguen para así desarrollar programas de defensa adecuados.

A. Características

La información que se genera simula tener un gran valor para las organizaciones, la misma que se utiliza para desarrollar métodos preventivos para evitar estos ataques.

Dispone de nuevas herramientas y tácticas que son diseñadas para capturar el tráfico que interactúa con ellos, con esto se provee un alto grado de detección de intrusos, de esta forma evitar que se den falsos positivos, es decir alertas falsas.

Tiene la capacidad de recopilar información de manera detallada de los intrusos internos y externos, lo que permite detectar potenciales riesgos sobre la red.

Se requiere de una dirección IP como mínimo para su funcionamiento.

B. Sistema de detección de intrusos

Un sistema de detección de intrusos (IDS, Intrusión Detection System) es uno de los componentes fundamentales de la seguridad actual de los sistemas. Actúa monitoreando el tráfico de la red para alertar al administrador de la presencia de actividades sospechosas.

Existen IDS que basan su sistema de detección de alertas en torno a la búsqueda de coincidencias con firmas específicas de amenazas conocidas, de manera similar al comportamiento de un software antivirus; mientras que otros, trabajan a partir de la detección de anomalías en el comportamiento de la red [3].

C. Ventajas y Desventajas de un Honeypot

1) Ventajas: Los Honeypots son una tecnología con un concepto muy simple y con una fortaleza muy poderosa.

Frente a un IDS [4], el Honeypot tiene una gran ventaja, ya que este permite la detección de nuevos tipos de ataques, a diferencia de un IDS que se basa

en reglas que ya están definidas para realizar la detección de los ataques conocidos.

Los recursos necesarios a utilizar son mínimos, de esta forma se puede implementar una plataforma lo suficientemente potente para operar a gran escala.

Trabaja en entornos sobre IPv6 [5], es decir, el Honeypot detectará un ataque sobre IPv6 de la misma forma que lo hace con un ataque sobre IPv4.

Generan información de mucho valor, cosa que no sucede con otros sistemas de seguridad que generan cientos de megas de ficheros Logs, con información que no es nada útil.

El tráfico cifrado dirigido a los sistemas Honeypot es fácil de analizar.

2) Desventajas: Como toda tecnología, los Honeypots también presentan 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.

Los Honeypots solo permiten rastrear y capturar actividad destinada a interactuar directamente con ellos, pues estas no capturan información relacionada a ataques destinados hacia otros sistemas vecinos, a menos que el atacante o la amenaza interactúe con el Honeypot al mismo tiempo.

Los Honeypots pueden llegar a constituir un riesgo potencial para la red, esto debido a la atracción que se genera a los posibles atacantes, es por ello que si no se configura adecuadamente el alcance del Honeypot y se lo convierte en un entorno controlado y cerrado, puede ser utilizado como punto de inicio para ataques a otras redes o incluso a la misma ubicación de los Honeypots en la red.

D. Ubicación de los Honeypot

Los Honeypots se pueden ubicar en la zona perimetral de la red de las organizaciones simulando una red interna; la ubicación de este dispositivo ha generado una gran controversia en la comunidad de profesionales de la seguridad.

La ubicación final del Honeypot dependerá principalmente de los requerimientos que tenga la organización basándose en los objetivos y metas del negocio.

A continuación mencionaremos diferentes opciones como sugerencia para ubicación de un Honeypot en la red de las organizaciones.

1) Honeypot antes del Firewall ver [6]: En esta ubicación es en la que menos riesgo se suministra a la red, ya que al encontrarse fuera de la zona protegida por el Firewall, puede ser atacado sin ningún tipo de peligro para el resto de la red.

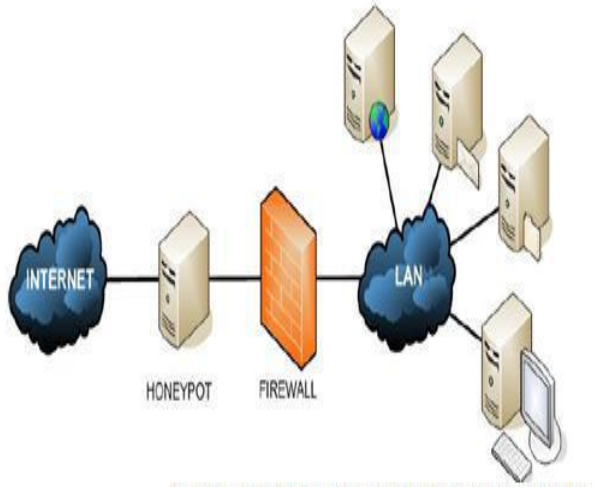

Fig.1 Ubicación de Honeypot antes del firewall [7].

2) Honeypot después del Firewall: En esta ubicación el acceso al Honeypot está dirigido por las reglas de filtrado del firewall, su ubicación permite la detección de los atacantes internos.

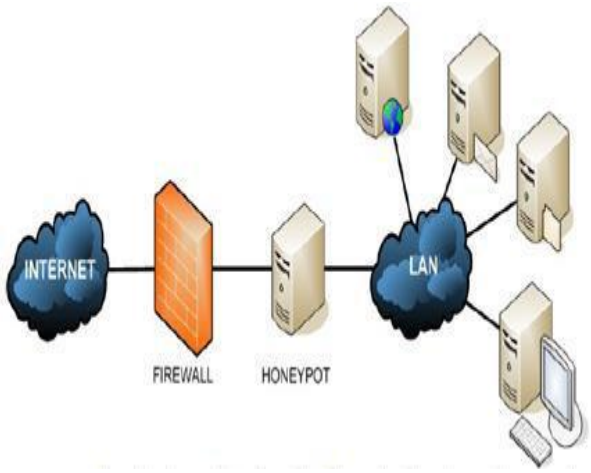

Fig. 2 Ubicación de una Honeypot después del firewall [7].

3) Honeypot en la zona desmilitarizada [7]: Esta es una de las mejores ubicaciones, ya que permite detectar ataques que se son externos e internos; para esto se requiere de una reconfiguración del Firewall.

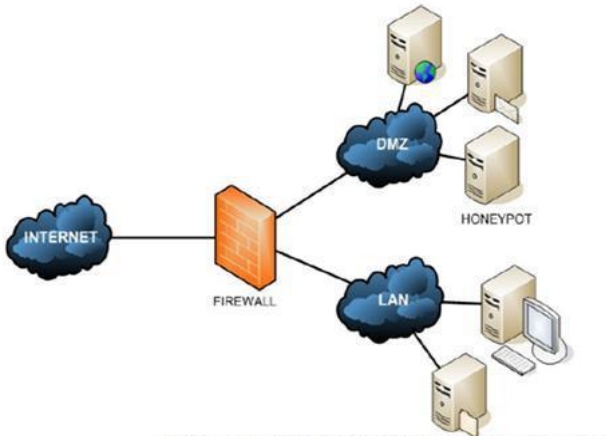

Fig. 3 Ubicación de un Honeypot en una zona desmilitarizada [7].

E. Tipos de Honeypot

1) Honeypots de Producción: Este tipo de Honeypot es diseñado principalmente para la seguridad y defensa de las redes. No han sido diseñados para recoger información sobre las actividades de Hacking, se implementa de manera colateral a las redes de datos o infraestructuras en ambientes reales y son utilizados para proteger a las organizaciones. Este tipo de Honeypot está sujeta a ataques constantes.

Actualmente a este tipo de Honeypot se le da más importancia debido a las herramientas de detección que se pueden utilizar, así como también por la forma cómo puede mejorar la protección en la red y de los servidores.

2). Honeypots para Investigación: Estos Honeypots son implementados con la finalidad de recolectar información sobre las acciones de los intrusos.

Por lo general son administrados por instituciones educativas sin fines de lucro y organizaciones de investigación, se utilizan para tener una visión más clara sobre las operaciones, estrategias y los motivos de ataques, estudiar patrones de ataque y amenazas de todo tipo.

El objetivo principal es identificar las amenazas y encontrar el modo de tratar con estas de una manera eficaz. Estos son difíciles de manejar y desplegar, pero son capaces de reunir una gran cantidad de información.

Existen otros tipos de Honeypot que permiten definir un rango de posibilidades de ataques de un potencial atacante, esto ayuda a entender no solo el tipo de Honeypot con el que se está trabajando, sino también ayuda a definir cuáles de las vulnerabilidades se necesitan que un atacante explote. Entre estos tipos tenemos los siguientes:

3). Honeypots de Baja Interacción: Este tipo de Honeypots trabajan únicamente emulando servicios y sistemas operativos. La actividad del atacante se encuentra limitada al nivel de emulación de la 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 [8].

El proceso de implementación de un Honeypot de baja interacción consiste en instalar un software de emulación de un sistema operativo, elegir el servicio a instalar, establecer una estrategia de

monitoreo y dejar que el programa opere por si solo de manera normal.

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.

Entre algunos ejemplos de Honeypots de baja interacción, [9] tenemos los siguientes:

Specter.
Honeyd.
KFSensor.
PatriotBox.
Bigeye.

4). Honeypots de Alta Interacción: Este tipo de Honeypots constituyen una solución compleja, ya que implica la utilización de sistemas operativos y aplicaciones reales montadas en hardware real sin la utilización de software de emulación e involucrando aplicaciones reales que se ejecutan de manera normal.

Con este tipo de Honeypot se tiene la posibilidad de capturar gran cantidad de información referente al modus operandi de los atacantes debido a que los intrusos se encuentran interactuando frente a un sistema real.

Los Honeypots de alta interacción no asumen responsabilidad sobre el comportamiento que tendrá el atacante, ya que se provee de un entorno abierto que captura todas las actividades realizadas, además ofrece una amplia gama de servicios, aplicaciones y depósitos de información que pueden servir como blanco potencial para aquellos servicios que se desea comprometer.

Esta capacidad también incrementa el riesgo que los atacantes puedan utilizar estos sistemas como entradas para lanzar ataques a sistemas internos que no forman parte de los Honeypots.

Una Honeynet (red señuelo) [10] es una red completa que ha sido configurada y conectada a otras redes para que pueda ser sondeada, atacada e incluso comprometida por intrusos.

F. Utilidades de las Honeypots

Las Honeypots son útiles para investigaciones forenses, ya que permiten analizar la actividad del Hacker o atacante basados en el engaño. Si ya se conoce la identidad del atacante y además se va a tomar acciones contra del atacante es importante recordar que antes de implementar una Honeypot se debe tener un permiso judicial.

Brindan protección, prevención, detección y respuesta a los ataques de baja interacción en sistemas de producción.

Facilitan la recolección de la información, esto ayuda a definir tendencias respecto a las actividades del atacante, activación de sistemas tempranos de alarma, predicción de ataques e investigaciones criminales con alta interacción.

G. Implicaciones Legales

Algunos de los problemas que se asocian al uso de las Honeypots se centran en el aspecto legal.

Los problemas principales que pueden acarrear estos sistemas incluyen la complicidad, protección de datos y responsabilidades por cualquier daño causado desde el Honeypot.

La tentativa generada por el uso de Honeypots es uno de estos problemas. Se podría pensar que el hecho de colocar un equipo en la red con la finalidad que sea comprometido, puede ser tomado como tentativa para comprometer otros sistemas, y fomentar la actividad maliciosa sobre la red, es decir se habilita el medio por el cual el intruso puede atacar a otros sistemas, sin embargo esto no es cierto, ya que la información obtenida de las Honeypots, es utilizada para un fin de investigación.

IV. ANALISIS Y RECOMENDACIONES.

Los Honeypots sirven como trampas para desviar la atención del atacante a la red de producción

evitando comprometer los principales recursos de información de las organizaciones, de igual manera, capturan códigos maliciosos para estudios posteriores. También, sirve para determinar el perfil del atacante y conocer sus métodos de intrusión, similar a la manera en que las investigaciones policiacas construyen el archivo de un criminal basado en su modo operandi.

Al momento de implementar un Honeypot en nuestras organizaciones, se presentan varios retos al administrador, uno de ellos, es la dificultad de descifrar como fue la metodología que implemento el atacante para ingresar, para esto se recomienda la utilización de un IDS como fuente de información y valor estadístico ya que este sistema por medio de firmas específicas de amenazas conocidas, podemos ver y analizar la arquitectura del ataque que se utilizó revisando sus alarmas emitidas, y así poder ver cuál fue la amenaza que el atacante exploto y con ello realizar un buen análisis de riesgo sobre la red y los controles de seguridad que tienen implementados; De esta manera brindar una mejor seguridad perimetral en las redes de las organizaciones.

Se sugiere, se usen arquitecturas de seguridad dinámicas para así conocer nuevas vulnerabilidades y riesgos de los distintos entornos computacionales.

V. CONCLUSIONES

Los Honeypots son un complemento global a los sistemas de seguridad y no una solución de seguridad, ya que estos proporcionan conocimiento para fortalecer los sistemas que se diseñen, y poder contrarrestar a los futuros atacantes que quieran ingresar ilegalmente a las organizaciones.

Un Honeypot es solo una herramienta, y la forma cómo se utiliza depende de quien la implemente y de cada organización según sus necesidades, ya sea para realizar investigación o simular un ambiente de producción.

Es una tecnología muy útil para la realización de cursos y laboratorios prácticos en especializaciones y maestrías de seguridad informática.

REFERENCIAS

[1] Internet World Satats. [En línea]. Disponible: http://www.internetworldstats.com/stats2.htm
[2] Todo acerca de cómo las computadoras [En Línea]. Disponible: http://www.compute-rs.com/es/consejos-84294.htm
[3] Akindeinde, O. (2009). Attack simulation and threat modeling. Lagos, Nigeria.
[4] Miguel José Hernández y López, Carlos Francisco Lerma Reséndez, *Aplicaciones Prácticas de los Honeypots en la Protección y Monitoreo de Redes de Información*.
[5] P. Diebold, A. Hess, G. Schafer, A Honeypot Architecture for Detecting and Analyzing Unknown Network Attacks.
[6] Fabien Pouget, Marc Dacier, Honeypot, Honeynet: A comparative survey.
[7] Honeypots: Herramienta de Seguridad de la Información [En línea]. Disponible: http://honeypots.wordpress.com/
[8] Robota. [En línea]. Disponible: http://www.robota.net/index.rsws?seccion=6&submenu=1&articulo=173.
[9] KeyFocus Products [En línea] .Disponible: http://www.keyfocus.net/kfsensor/
[10] Álvaro Gómez Vieites, *Enciclopedia de la Seguridad Informática, Alfaomega Grupo Editor, México, 2007.*

Eduard Arenas, Ingeniero Electrónico egresado de la Universidad de Pamplona, actualmente labora en una cadena hotelera, en el departamento de Tecnologías de la Información bajo el cargo de Analista de seguridad e Infraestructura

Daniel López, Ingeniero de Sistema egresado de la institución Universitaria Politécnico Grancolombiano, actualmente labora en la Dirección de Impuestos y Aduanas Nacionales-DIAN en el área de Gestión de Tecnología de Información y Telecomunicaciones.