HONEYPOTS

Boris Coronel Salazar
Universidad Mayor De San Andrés
Carrera Informática
Análisis y Diseño de Sistemas de Información
willcs77@hotmail.es

RESUMEN

En el artículo se especificará la relación importante que existe entre “Ethical Hacking” y los honeypots. Existen varios tipos de HONEYPOTS al igual que varios propósitos en su uso. La investigación nos lleva a encontrar cuando fue usado por primera vez. También se realizo una investigación para determinar la incidencia de ataques que podría sufrir un ordenador típico. En particular se hablar de Ghost (honeypot). Se hablará de las estrategias que se usa para atrapar a los hackers y spammers dentro de esta trampa.

Palabras Clave

Ghost, Honeypot, Ethical Hacking, Hackers.

1. INTRODUCCION

El término honeypot fue acuñado durante la Guerra Fría para designar una técnica de espionaje y hasta comienzos de la década de los 90 no comienza a utilizarse en el campo de la seguridad de la información.
El libro de la figura explica muy detalladamente los diferentes usos de los honeypots.

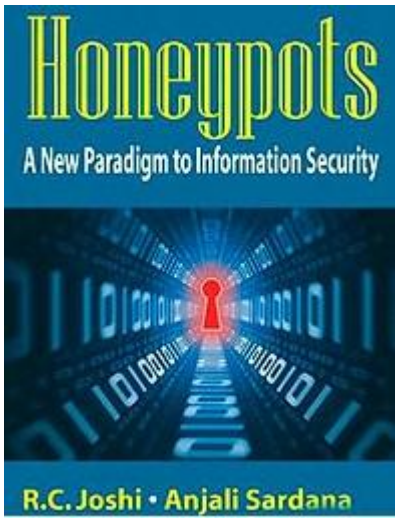

Figura 1. Uno de los libros de honeypots

En Seguridad Informática un honeypot es un recurso que no se ha diseñado para recibir tráfico legítimo, sino para aparentar servicios, sistemas operativos o incluso redes enteras, que puedan resultar atractivos para un eventual atacante y que presenten vulnerabilidades fáciles de explotar, alejando al intruso de los recursos reales a la vez que monitorizan todo esa actividad malintencionada.

"En la terminología informática, un ***honeypot*** es una trampa para detectar, desviar o de alguna manera contrarrestar los intentos de uso no autorizado de los sistemas de información." Honeypot atraer un hacker en un sistema tiene varios propósitos:
- El administrador puede ver los hackers explotan las vulnerabilidades del sistema, con lo que aprender que el sistema tiene debilidades que necesitan ser rediseñado.

- El hacker puede ser capturado y detenido al intentar obtener acceso de root al sistema.

- Mediante el estudio de las actividades de los hackers, los diseñadores pueden crear mejores sistemas más seguros que son potencialmente invulnerable a los futuros hackers.

Hay dos tipos principales de honeypots:

Producción - Un honeypot es la producción que se utiliza en el entorno de una organización para ayudar a mitigar los riesgos.

Investigación - Un sistema de este tipo agrega valor a la investigación en seguridad informática, proporcionando una plataforma para estudiar la amenaza

Otros tipos de Honeypots: Su objetivo es desarrollar un sistema en el cual todas las actividades sean controladas y seguidas.

- *Honeyd* (baja interacción) - un demonio con licencia GPL, que es capaz de simular grandes estructuras de red en un único host.

- *Mwcollect*, Nepenthes (Mediano-interacción) - Honeypot donde el malware infecta un entorno simulado

- *Spam honeypots* - Honeypot programas creados por los administradores, que se disfrazan de recursos abusable con el fin de descubrir las actividades de los spammers.

- *E-mail trampa* - Una dirección de correo electrónico que no se utiliza para ningún otro propósito que el de recibir correo no deseado también se puede considerar un honeypot spam.

Una investigación realizada el 2006 demostró las incidencias de ataques que podría sufrir un ordenador típico los cuales son:

En una primera fase, consistente en simplemente registrar el número y tipo de ataques, los resultados fueron que cada 15 minutos, como media, el ordenador recibía spam «molesta», típicamente ofertas fraudulentas para mejorar la seguridad del ordenador. Sin embargo, cada hora, como media, el ordenador

recibía ataques más serios, de gusanos informáticos tipo SQL.Slammer y MS.Blaster.[1]

La segunda fase de la investigación consistía en dejar entrar el *adware* y *spyware* para ver sus eventuales efectos en el ordenador. El resultado fue que, de tratarse de un ordenador cualquiera en un hogar normal, hubiera quedado totalmente insegura e inservible.

2. EL GHOST (HONEYPOT)

Ghost es un honeypot de malware que se propaga a través de dispositivos de almacenamiento USB.Detecta las infecciones por este tipo de malware sin la necesidad de cualquier otra honeypot information. Fue desarrollado por primera vez para una tesis de licenciatura en la Universidad de Bonn en Alemania.Ahora el desarrollo se continúa por el mismo desarrollador dentro del Proyecto Honeynet.
Es un honeypot de malware USB.Es capaz de capturar el malware que se propaga a través de dispositivos de almacenamiento USB sin ningún conocimiento más allá.Esto se hace mediante la emulación de una unidad flash USB y engañar el malware en infectar el dispositivo emulado.Debido al hecho de que la máquina debe estar infectada con el fin para el dispositivo virtual para detectar el malware, el honeypot está diseñado para funcionar en sistemas Windows, que se dirige principalmente por el malware en el momento.

Figura 2. Malware (GHOST)

Actualmente, sólo es compatible con Windows XP y se encuentra en una etapa temprana de desarrollo, aunque su concepto se ha demostrado que funciona bien, y el código es
estable.Si Ghost detecta una infección, entonces actualmente sólo informa de que la máquina está posiblemente infectada, sin incluir ninguna información adicional.

3. SPAM HONEYPOTS

Los *spammers* son usuarios que abusan de recursos como los servidores de correo abiertos y los proxies abiertos. Algunos administradores de sistemas han creado *honeypots* que imitan este tipo de recursos para identificar a los presuntos *spammers*.

Figura 3. Spammers

Algunos *honeypots* Jackpot, escrito en Java, y smtpot.py, escrito en Python. Proxypot es un *honeypot* que imita un proxy abierto (o *proxypot*).

4. HONYPOTS DE SEGURIDAD

Programas como *Deception Toolkit* de Fred Cohen se disfrazan de servicios de red vulnerables. Cuando un atacante se conecta al servicio y trata de penetrar en él, el programa simula el agujero de seguridad pero realmente no permite ganar el control del sistema. Registrando la actividad del atacante, este sistema recoge información sobre el tipo de ataque utilizado, así como la dirección IP del atacante, entre otras cosas.

4.1 Honeynet Project

Es un proyecto de investigación que despliega redes de sistemas *honeypot* (*HoneyNets*) para recoger información sobre las herramientas, tácticas y motivos de los criminales informáticos.

4.2Security

Suite es un proyecto que desarrolla una Suite de Seguridad Informática. Dentro de los programas que la engloban está disponible un Honeypot configurable de baja interacción. El proyecto es multiplataforma, programado en Ruby y esta licenciado bajo GNU/GPL.

5. CONCLUSIONES

El estudio de los HONEYPOTS es muy complejo de hecho su estudio y aplicación se aboca más a las grandes empresas pero con el tiempo ha evolucionado en su uso.

6. REFERENCIAS

1. [1]Cual es el propósito de los Honeypots[Disponible en:]
http://ethics.csc.ncsu.edu/abuse/hacking/honeypots/study
[Fecha de búsqueda:] 19/04/13

[2] Hacking honeypots [Disponible en:]
http://ethics.csc.ncsu.edu/abuse/hacking/honeypots/study
[Fecha de búsqueda:] 19/04/13

[3] Honeypots: Un nuevo paradigma para la seguridad
[Disponible en:]
http://www.soyforense.com/2011/10/06/honeypots
[Fecha de búsqueda:] 19/04/13

[4] Soluciones de software atómica [Disponible en:]