

Aplicaciones Prácticas de los Honeypots en la Protección y Monitoreo de Redes de Información

Miguel José Hemández y López
*Unidad Académica Multidisciplinaria de Comercio y Administración -
Victoria*
miguel@honeynet.org.mx

Carlos Francisco Lerma Reséndez, MSc
Dirección General de Innovación Tecnológica - UAT
cflerma@honeynet.org.mx

Introducción

Toda organización que considere las Tecnologías de Información (TIs) como la espina dorsal de su estructura operativa debe estar a la vanguardia en sus procesos de cambio, debido a que disponer de información confiable y a tiempo constituye una ventaja fundamental. La identificación de los riesgos a los cuales está sujeta la información corporativa es de vital importancia para asegurar la integridad, usabilidad y utilidad de la misma.

Tradicionalmente, la naturaleza del ramo de la Seguridad Informática ha sido puramente defensiva. Los muros de fuego, sistemas de detección de intrusos, y el cifrado son mecanismos que se usan defensivamente para proteger los recursos informáticos. Los dogmas estratégicos de la Seguridad Informática consisten en defender la infraestructura de información tan bien como sea posible, detectar posibles fallos en la estructura defensiva y reaccionar a esos fallos de manera proactiva. La naturaleza de la existencia y operación del enemigo informático es puramente defensiva, ya que éste siempre está al ataque.

Los Honeypots han demostrado su valor como herramienta de investigación en el área de la seguridad de la información. Muchos investigadores y organizaciones, tanto públicas como privadas, que forman parte de la comunidad de la seguridad están utilizando actualmente redes “trampa” para aprender las tácticas, técnicas y los procedimientos que la comunidad “hacker” utiliza para irrumpir de manera no autorizada a bóvedas de información electrónica que podrían contener información potencialmente sensible. Este artículo analiza el funcionamiento de los honeypots y su tecnología, que se está

convirtiéndolo en el componente clave del sistema de capas de protección contra intrusos.

Honeypots – Que son y como funcionan

Los Honeypots son una tecnología nueva con enorme potencial para la comunidad informática. Los primeros conceptos fueron introducidos por primera vez por varios íconos en la seguridad informática, especialmente aquellos definidos por Cliff Stoll en el libro "The Cuckoo's Egg" y el trabajo de Bill Cheswick documentado en el libro "An Evening with Berferd". Desde entonces, han estado en una continua evolución, desarrollándose de manera acelerada y convirtiéndose en una poderosa herramienta de seguridad hoy en día.

Los Honeypots son en su forma más básica servidores de información falsos, posicionados estratégicamente en una red de prueba, los cuales son alimentados con información falsa que es disfrazada como archivos de naturaleza confidencial. A su vez, estos servidores son configurados inicialmente de manera que sea difícil mas no imposible el hecho de ser penetrados por un atacante informático, exponiéndolos de manera deliberada y haciéndolos altamente atractivos para un "hacker" en busca de un blanco. Por último, el servidor es habilitado con herramientas de monitoreo y rastreo de información, de manera que cada paso y rastro de actividad de un "hacker" pueda ser registrado en una bitácora que indique esos movimientos de manera detallada.

Las funciones principales de un Honeypot son:

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

En un contexto más avanzado, un conjunto de Honeypots forma una Honeynet, proporcionando así una herramienta que abarca un conjunto extendido de posibles amenazas y proporciona al administrador de sistemas mayor información para su estudio. Inclusive, hace más fascinante el ataque para intruso debido a que se incrementan las

posibilidades, blancos y métodos de ataque.

Clasificación de los Honeypots

Los Honeypots se pueden clasificar de acuerdo a dos criterios: Según su Ambiente de Implementación y según su Nivel de Interacción. Estos criterios de clasificación hacen fácil entender su operación y utilización al momento de planear la implementación de uno de ellos dentro de una red de datos o infraestructura de TIs.

Honeypots según su Ambiente de Implementación

Bajo esta categoría podemos definir dos tipos de Honeypots: Para la Producción y para la Investigación.

Honeypots para la Producción: Son aquellos que se utilizan para proteger a las organizaciones en ambientes reales de operación. Se implementan de manera colateral a las redes de datos o infraestructuras de TIs y están sujetas a ataques constantes las 24 horas del día, 7 días a la semana (24/7). 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 los hosts.

Honeypots para la Investigación: Estos Honeypots no son implementados con la finalidad de proteger redes, sino que constituyen recursos educativos de naturaleza demostrativa y de investigación cuyo objetivo se centra en estudiar patrones de ataque y amenazas de todo tipo. 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.

Honeypots según su Nivel de Interacción

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, éstos 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 soportará 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 sí 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, esa 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.

Ventajas y desventajas

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.

Los Honeypots pueden ayudar a prevenir ataques en varias formas:

- Defensa contra ataques automatizados: Estos ataques son basados en herramientas que aleatoriamente 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 los 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 continua. 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 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 logeo 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(s) de sus servidores fue(ron) comprometido(s) 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 ayudan 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.

Bibliografía

- [1] HoneyNet Project, <http://www.honeynet.org>
- [2] HoneyNet Project México, <http://www.honeynet.org.mx>
- [3] HoneyNet Project, *Know Your Enemy: Learning about Security Threats (2nd Edition)*, 2005
- [4] Spitzner Lance, *Honeypots: Tracking Hackers*, 2002
- [5] Dunsmore B., Brown J. and Cross M., *Mission Critical!: Internet Security*, 2002
- [6] Man Young Rhee, *Internet Security*.
- [7] HoneyNet Project, *Know your Enemy: Honeynets*, <http://www.honeynet.org/papers/honeynet/index.html>
- [8] Philippine HoneyNet Project, *Honeynets Learning*, 2006
<http://www.philippinehoneynet.org/docs/honeynetlearning.pdf>
- [9] Roberti, Raquel y Bonsembiante, Fernando. *Llaneros solitarios. Hackers, la guerrilla informática*.
- [10] Hassan Artaila, Haidar Safab, Malek Sraja, Iyad Kuwatlya, Zaid Al-Masria, *A hybrid honeypot framework for improving intrusion detection systems in protecting organizational networks*, 2006
- [11] Fabien Pouget and Thorsten Holz, *A Pointillist Approach for Comparing Honeypots*
- [12] HoneyD, <http://www.honeyd.org>
- [13] The HoneyNet Project. *Know Your Enemy: GenII Honeynets*, 2003.
<http://www.honeynet.org/papers/gen2/>
- [14] Corrado Leita¹, Marc Dacier¹ and Frederic Massicotte, *Automatic Handling of Protocol Dependencies and Reaction to 0-Day Attacks with ScriptGen Based Honeypots*

[15] Provos, N.: *A virtual honeypot framework*. In: Proceedings of the 12th USENIX Security Symposium, 2004

[16] Stephan Riebach, Erwin P. Rathgeb, and Birger Toedtman, *Efficient Deployment of Honeynets for Statistical and Forensic Analysis of Attacks from the Internet*

Acerca de los autores:

Miguel José Hernández y López <miguel@honeynet.org.mx> es miembro fundador y líder del Proyecto Honeynet México. Ha sido ponente invitado en diversos congresos de software libre y seguridad informática en México y en el extranjero, entre las cuales se incluye una notable participación en las 6as. Jornadas de Software Libre de la Universidad de Mendoza, Argentina.

Carlos Francisco Lerma Reséndez, MSc <cflema@uat.edu.mx> es ingeniero de servicio a cargo del área de Monitoreo de Tecnologías de Información en la Dirección de Informática y Telecomunicaciones, perteneciente a la Dirección General de Innovación Tecnológica de la Universidad Autónoma de Tamaulipas. Egresó de la carrera de Contador Público de la Unidad Académica Multidisciplinaria de Comercio y Administración – Victoria y es Maestro en Ciencias en Administración de Telecomunicaciones y Redes por Syracuse University en Syracuse, New York.