



Señuelos y máquinas trampa: conozca a su enemigo



En “El Arte de la Guerra”, Sun Tzu resume las claves de la victoria en una frase: “Conoce a tu enemigo”. Dicha frase se ha convertido en el estandarte de toda una nueva generación de expertos en seguridad y de desarrolladores de producto especializados, dedicados a aprender las técnicas y herramientas que “nuestros enemigos” escojen.

Román Ramírez

Introducción

La tecnología de seguridad a pesar de ser, probablemente, la que más rápida actualización necesita, suele ir algunos pasos por detrás de las técnicas que los potenciales atacantes conocen.

Sabemos que cuentan con acceso a las vulnerabilidades antes, incluso, que listas especializadas como Bugtraq, VulnWatch o Secunia (muchos atacantes intercambian vulnerabilidades que ellos llaman de “zero-day” o “día cero” en castellano).

Este retraso en el conocimiento de problemas o técnicas de seguridad, generalmente nos deja expuestos a ataques desconocidos, nuevos gusanos de distribución masiva o nuevas herramientas.

La filosofía de las herramientas conocidas como “honeypot” (tarros de miel, en traducción literal) es innovadora desde la perspectiva de la seguridad tradicional, y abre un frente infinito de posibilidades en el aprendizaje, convirtiendo la mejora de nuestra seguridad en una evolución activa y no la actual respuesta pasiva-defensiva.

El concepto de honeypot es extremadamente sencillo; uno puede dejar un tarro de miel en el bosque esperando que un oso se vea atraído por tan suculento manjar, y una vez éste ha introducido su hocico dentro, podemos soltar nuestra red y capturarlo.

Y de la misma manera, podemos insertar un equipo “trampa” en nuestra estructura de red actuando como ese tarro de miel para llamar la atención de los atacantes y lanzarles la trampa una vez hayan entrado.

Tarpit

Antes de la aparición del concepto de tarro de miel (honeypot), profesionales

del mundo de la seguridad como Tom Liston, desarrollaron una idea ingeniosa para bloquear y controlar ataques de gusanos como CodeRed y CodeRedII.

LaBrea, un “tarpit” (pozo de alquitrán en inglés), apareció como un producto inteligente, que simulaba ser un servidor web vulnerable al ataque de CodeRed, y

caciones como LaBrea; pensemos en herramientas de detección de intrusos, que al detectar un patrón conocido de ataque puedan mantener al atacante conectado, haciéndole creer que, simplemente, la conexión va lenta.

HoneyPot

El concepto del honeypot, aunque no fue inventado por el “Proyecto HoneyNet”, es en éste donde ha desarrollado toda su entidad, evolucionando hasta convertirse en una serie de documentos y herramientas útiles y aplicables incluso dentro del mercado profesional.

Como antes se comentaba, un honeypot es un equipo que simula ser una máquina en servicio completamente normal, y que tiene como objetivo seguir el rastro de cada acción que potenciales atacantes puedan efectuar sobre él.

Ese tiempo de desventaja que todos los expertos en seguridad tenemos frente a los atacantes, puede ser compensando con un conocimiento exhaustivo de sus técnicas y herramientas. ¿Qué valor le daríamos a los planos detallados de las armas especializadas de un criminal?

Uno de los tópicos a los que más nos aferramos es al de que no sufriremos un ataque, ya que nuestra red es desconocida y de poco interés para un potencial atacante. Nada más lejos de la realidad, como viene a demostrar uno de los primeros documentos en el “Proyecto HoneyNet”: el ataque más rápido que han recibido se produjo quince minutos después de que hubieran conectado una máquina por primera vez, y el tiempo medio que han calculado, es de más o menos una hora antes de recibir el primer ataque.

Creo que todos los que tenemos un cortafuegos personal instalado, observamos el número de intentos de conexión que recibimos “simplemente leyendo el correo”.

En la creación de un honeypot se pueden tomar diferentes aproximaciones, todas ellas válidas siempre que se gestionen correctamente. Muchas de estas aproximaciones se toman por una limitación en la inversión, y demuestran un gran ingenio en la construcción de herramientas muy potentes con un coste mínimo.

Una primera aproximación es la de instalar una máquina dedicada, con un sistema operativo no asegurado, y apli-

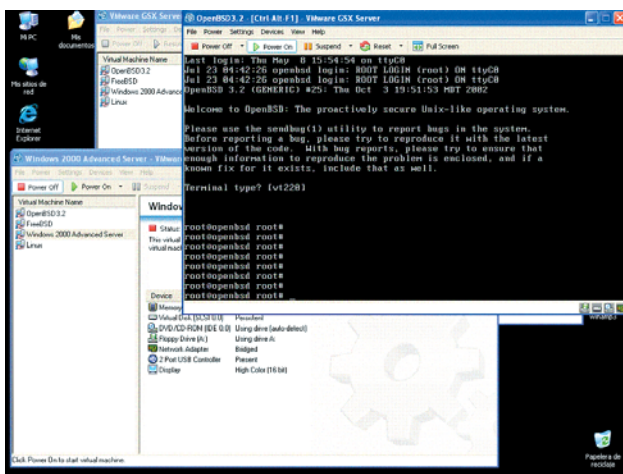


Figura1.- VMware en funcionamiento: OpenBSD y otros sistemas arrancados en una HoneyNet.

La filosofía de las herramientas conocidas como “honeypot” es innovadora desde la perspectiva de la seguridad tradicional y abre un frente infinito de posibilidades en el aprendizaje, convirtiendo la mejora de nuestra seguridad en una evolución activa y no la actual respuesta pasiva-defensiva.

que, en el momento que recibía una conexión del gusano, le mantenía “enganchado” a la conexión, obteniendo dos objetivos inmediatos: el primero, detener el ataque del gusano, ya que nuestro “alquitrán” le mantenía “pegado”, y segundo, facilitar la localización de los atacantes, exactamente por el mismo motivo.

La idea del pozo de alquitrán donde uno se queda pegado es muy interesante, ya que no es aplicable únicamente a apli-



cando las debidas medidas de control, conectarla a la red y esperar el incidente. Este tipo de instalación de una máquina real dedicada se conoce como de "Honeypots clásicos".

Esta primera filosofía implica tener mucho cuidado en lo que se refiere a proteger al resto del mundo, en caso de que nuestra máquina sufra un compromiso (uno de los objetivos de los atacantes es obtener acceso a máquinas que les puedan servir como reflectores o repetidores de un ataque). El tiempo que no invertimos en preparar aplicaciones específicas, lo invertiremos en configuraciones de cortafuegos y medidas de control del sistema operativo, herramientas de captura externas.

Si el atacante consigue éxito en su intrusión debemos asegurarnos de vetar cualquier potencial ataque a terceros desde nuestro sistema en estudio.

Otra aproximación es crear sistemas operativos simulados con herramientas como VMWare, Bochs, Linux Virtual System o la capacidad de crear "cárceles" (*Jail*) con los sistemas BSD.

Esta filosofía facilita el añadir nuevas trampas, que pueden ser incorporadas al laboratorio de forma inmediata y sin detener el servicio de las demás.

Herramientas como Honeyd -una aplicación que permite construir nuestro propio honeypot con cierta facilidad sobre cualquier plataforma Unix, o el propio LaBrea-, son ejemplos clásicos de aplicaciones especializadas de honeypot. Esta filosofía de simulación de sistemas se conoce como de "Honeyd virtuales".

Otra característica importante de las herramientas de honeypot es la de controlar el nivel de interacción del intruso con la trampa.

Las herramientas de "baja interacción" limitan al atacante a operar exclusivamente con los servicios simulados, lo que hace que el nivel de riesgo a asumir instalando la trampa sea menor, mientras que los honeypot de "alta interacción" le permiten acceder al intérprete de comandos, en muchas ocasiones una práctica arriesgada. Algunos honeypot virtuales pueden simular el acceso al intérprete de comandos convirtiéndose en trampas mejoradas, aunque de "baja interacción" (reduciendo los riesgos).

HoneyNet

La evolución lógica de los honeypot son las honeyNet (una red tarro de miel).

En este caso, diseñamos y construimos la simulación de una red completa, utilizando herramientas que permitan controlar y gestionar tanto los sistemas como las evidencias que podemos obtener.

La recomendación ideal es utilizar herramientas como VMWare, que permiten simular diferentes máquinas y sistemas operativos, con sus diferentes direcciones ip y servicios.

Un ejemplo podría ser una simulación de la red completa de una empresa pequeña, con un servidor web, un servidor de correo y un servidor de ficheros, que podrían ser fácilmente emulados en un único ordenador compatible, manteniendo la apariencia de ser tres equipos completamente diferentes.

que, cuando nuestras herramientas detecten un acceso, sabremos a ciencia cierta que hay un motivo no muy limpio detrás de este acceso.

Por ejemplo, podemos crear un documento con cifras económicas falsas, y depositarlo en un almacén de documentos con un nombre llamativo para un potencial atacante, de forma que, cuando se produzca un acceso sobre este documento, habremos detectado a un potencial intruso.

La aplicación más común de la idea de honeytoken es la detección de herramientas de análisis de red (*sniffer*) con trampas.

En muchas ocasiones, detectar un sniffer en la red es una tarea imposible y hay que recurrir a trucos basados más en la astucia que en la tecnología.

Uno de estos trucos es crear un par usuario y contraseña falsos para acceder a un sitio de red falso, y lanzarlos por la red que sabemos está siendo espía. En un alto porcentaje de los casos, el espía hará uso de este usuario y contraseña, cayendo en nuestra trampa.

Análisis forense

La ciencia de análisis forense aplicada a la informática cuenta con un gran aliado en las herramientas de honeypot. En un gran número de casos, el experto forense cuenta con escenas del crimen corruptas o manipuladas, lo que sitúa el valor de las evidencias en como mínimo dudosas.

Pero, conociendo el comportamiento típico de un atacante—que generalmente siempre intenta volver a introducirse en el sistema comprometido—, se pueden construir una serie de trampas que capturen todas las evidencias en un nuevo ataque, incluso añadiendo la presencia de un notario que de fe de que se han cumplido todos los procedimientos y metodologías.

En EE.UU. actualmente hay un debate serio sobre la legalidad de las herramientas de honeypot, e incluso se han llegado a presentar denuncias en el estado de Michigan contra el uso de herramientas "espía" en las comunicaciones de atacantes.

En nuestro país, la legislación permite la utilización con ciertos límites de este tipo de herramientas, aunque conforme su popularidad vaya creciendo se revisará, buscando cubrir potenciales lagunas.

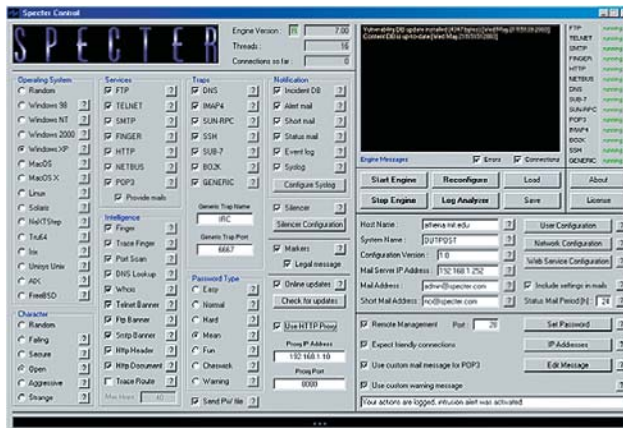


Figura 2. - Pantalla de Specter 7.0

La evolución lógica de los honeypot son las "honeyNet": en este caso, se diseña y construye la simulación de una red completa utilizando herramientas que permitan controlar y gestionar tanto los sistemas como las evidencias que puedan obtenerse.

Honeytoken

El término honeytoken fue acuñado por Augusto Paes de Barros en este mismo año 2003, y fue añadido a la lista de términos oficiales del "Proyecto HoneyNet" de inmediato. La idea de los honeytoken (piezas de miel, sería la traducción literal) se lleva utilizando largo tiempo, y ya en un anterior artículo sobre Informática Forense de esta revista (véase SIC nº 54) dimos un ejemplo.

El honeytoken es un documento, fichero, recurso o elemento accesible a través de la red, que tiene como único propósito el ser accedido por un potencial intruso o atacante. Obviamente, garantizaremos que ningún acceso autorizado se realizará sobre este elemento, de manera



Experto en elaboración de perfiles (profiler)

Como cierre de la parte descriptiva de este artículo, no podemos olvidar mencionar una nueva disciplina que ha nacido de la mano del "Proyecto HoneyNet": la elaboración de perfiles (*profiling* en inglés).

Esta nueva disciplina se dedica a analizar las evidencias obtenidas en incidentes de seguridad, y elaborar perfiles psicológicos, de carácter, actitud, conocimientos e intereses de los atacantes involucrados.

De la misma manera que las fuerzas de la ley tradicional analizan la figura del criminal intentando conocerle, los expertos en elaboración de perfiles intentan conocer a su atacante virtual.

El mundo comercial y el mundo "abierto"

Como siempre en todos los desarrollos en Internet, y con mucha más importancia en el mercado de la seguridad, existen soluciones comerciales y "abiertas" indistintamente.

La solución más común que se suele implantar es la de un equipo de bajo coste, con OpenBSD (por su nivel de seguridad), Snort (el detector de intrusos), Sebek2 (una herramienta que captura todas las pulsaciones tecleadas dentro de un sistema) y generalmente herramientas como tcpdump (una herramienta de captura de tráfico).

En el mundo comercial hay iniciativas lanzadas, como por ejemplo la de Enterasys con un módulo de *honeypot* para su detector de intrusos, Dragon.

En este contexto, hemos podido probar Specter 7.0, un detector de intrusos y *honeypot* para sistemas Microsoft, y la verdad, su filosofía parece interesante (aunque la plataforma no creemos que sea la más adecuada para una herramienta de este tipo).

Specter puede simular hasta catorce tipos de sistema operativo (incluyendo Linux, BSD, Solaris, Windows y otros), y además cuenta con una filosofía de simulación de nivel de seguridad que permite al usuario configurar cómo de abierta quiere la trampa.

Conocemos también KFSensor de Keyfocus y aunque no lo hemos podido probar, hay características interesantes. Este producto también es para plataforma Microsoft.

Conclusiones

Al margen de consideraciones tecnológicas, las herramientas de *honeypot*

provocan un gran número de reflexiones en su aplicación.

En EE.UU. ya se han dado casos en los que un atacante reclama la autoría de una intrusión en un sistema y la organización propietaria del sistema contesta con orgullo enseñando su *honeypot*. ¿Puede ser esta una práctica común en la gestión de la imagen de la empresa? "Si sufrimos un incidente, la postura oficial de la empresa es que se trataba de un *honeypot* y asunto zanjado".

Por otro lado, ¿cuántos responsables de seguridad pueden correr el riesgo de introducir una máquina en su red para

surgir sobre la validez de las evidencias obtenidas mediante una "trampa". ¿Son válidas ese tipo de pruebas? Dentro de las fuerzas de la ley hay opiniones divergentes.

Nuestra apreciación personal es que estas herramientas tienen una utilidad muy grande en la protección y prevención, y su implantación cada día se hace más necesaria, teniendo en cuenta lo rápido que evolucionan las técnicas de los atacantes.

Aún contando con los problemas derivados de su uso, los *honeypot* dan un aporte tal de información que difícilmente puede concebirse el actual nivel de seguridad sin ellos (es gracias a iniciativas como "Proyecto HoneyNet" que muchos problemas masivos han sido detenidos en su inicio).

Por la propia evolución del mercado de la seguridad, estamos convencidos de que en menos de tres años vamos a ver grandes instalaciones incorporando herramientas con estas características, de forma que puedan aprender dinámicamente de sus "enemigos" en Internet. ■

ROMÁN RAMÍREZ GIMÉNEZ
Gerente de Seguridad de Sistemas
AFI
roman_ramirez@afiglobal.com

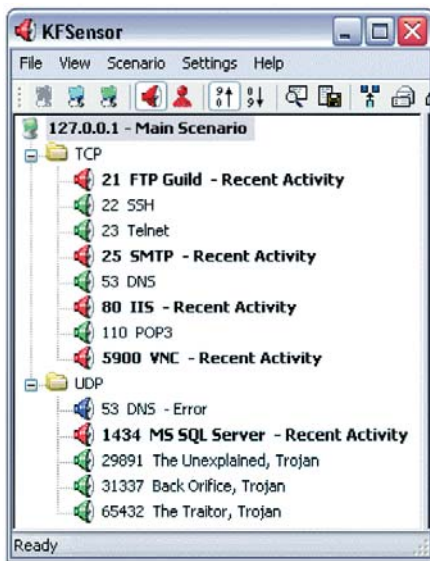


Figura 3.- KF Sensor

La elaboración de perfiles es la nueva disciplina nacida del "Proyecto HoneyNet", dedicada a analizar las evidencias obtenidas en incidentes de seguridad, y elaborar perfiles psicológicos, de carácter, actitud, conocimientos e intereses de los atacantes involucrados.

que su función sea la de ser atacada? Todos conocemos cuál es la política de muchas organizaciones frente a los incidentes de seguridad: negarlos. Realmente, ¿este tipo de organizaciones se arriesgarían a introducir un elemento que les podría poner en primera página de los periódicos al día siguiente?

Otra cuestión importante es que una mala configuración de un *honeypot* puede dejar a una organización en manos de un atacante, precisamente porque se le había facilitado el acceso.

Y no olvidemos las dudas que pueden

REFERENCIAS Y ENLACES

- LaBrea**, por Tom Liston
<http://www.hackbusters.net>
- Proyecto HoneyNet**
<http://www.honeynet.org>
- Traducción del Proyecto HoneyNet**
http://his.sourceforge.net/proy_his/index.php
- Honeyd**, por Niels Provos
<http://www.citi.umich.edu/u/provos/honeyd/>
- Extracto del código penal de Michigan**
<http://www.michiganlegislature.org/printDocument.asp?objName=mcl-750-540c&version=txt>
- "Honeyd: tracking hackers"**, Lance Spitzner, ISBN: 0-321-10895-7
- "Hacker's Challenge"**, Mike Schiffman y otros, ISBN: 0-07-219384-0
- Honeytokens**, por Lance Spitzner
<http://www.securityfocus.com/infocus/1713>
- Construyendo una HoneyNet Virtual**
http://www.linuxsecurity.com/feature_stories/feature_story-100.html
- Specter**
<http://www.specter.com>
- KF Sensor**
<http://www.keyfocus.net/kfsensor/>