Honeypot

Servidores Web de Altas Prestaciones (SWAP)

Miguel González Contreras

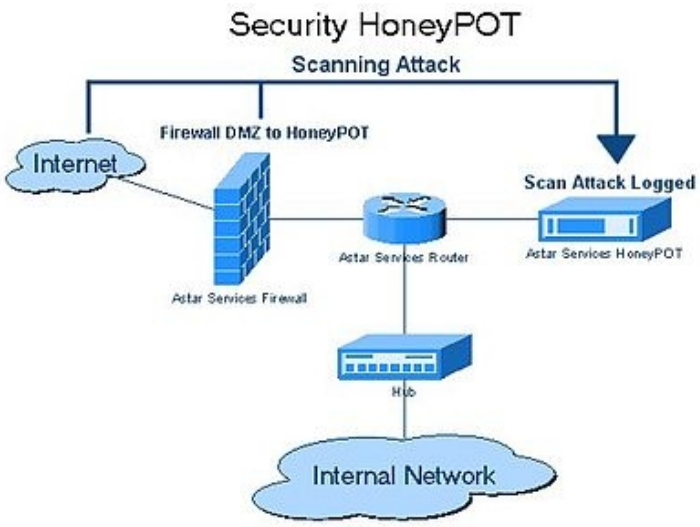
05/05/2019

Índice

1. ¿Qué es un honeypot?

Un ***honeypot***, o sistema trampa o señuelo, es una herramienta de seguridad informática dispuesto en una red o sistema informático para ser el objetivo de un posible ataque informático, y así poder detectarlo y obtener información del mismo y del atacante. El término *honeypot* significa en inglés, literalmente, "tarro de miel". Sin embargo, tanto en el Reino Unido como en Estados Unidos han usado este término para referirse a otras cosas, relacionando siempre sarcásticamente con un tarro de miel. Así, lo han usado para referirse a algo tentador que resulta ser una trampa.

Lo que hace es que mediante un software o a través de la acción humana, el *honeypot* hace que una empresa simule tener algunas "puertas de entrada" a sus sistemas que no han sido suficientemente protegidas.



Podemos decir, que es un gran aliado para defender tu red, aunque el concepto sea atraer ataques, la mejor táctica para defenderse es saber cómo actúa el enemigo y qué mejor que ponerle un cebo el cual no supondrá un riesgo para nuestra red, y nos ayudará a saber cómo incide el ataque y de qué manera.

2. ¿Cómo funciona?

La táctica es la siguiente. De manera previa, una empresa decide habilitar una serie de servidores o sistemas cuyo aspecto parezca sensible. Aparentemente, esa empresa se ha dejado varios cabos sin atar y parece vulnerable. Una vez dejada la trampa, la intención es atraer al atacante, que acudirá a la llamada para intentar entrar. Sin embargo, lo que el cibercriminal no sabe es que, lejos de estar encontrando una puerta vulnerable, en realidad está siendo perfectamente controlado y monitorizado por la empresa en cuestión.

De este modo, las empresas obtienen un beneficio triple:

- En primer lugar: contener posibles ataques verdaderamente peligrosos.
- En segundo lugar: entretener y desgastar al atacante haciéndole perder el tiempo.
- En tercer lugar: analizar sus movimientos para detectar posibles nuevas formas de ataque que se estén llevando a cabo en el sector.

El honeypot es similar al llamado contraespionaje de ciberseguridad, que también opta por colocar señuelos de ciberseguridad que, aparentando ser vulnerables, consigan atraer a los atacantes para engatusarlos y frenar sus ataques a la vez que espían, analizan y monitorizan todos sus movimientos.

De hecho, existen formas de sofisticar aún más el asunto: si el *honeypot* no se desarrolla sobre redes sin usar, sino sobre aplicaciones y sistemas totalmente reales, hablaremos de otro concepto, el de *honeynet*, que conseguirá engañar aún más al cibercriminal y hacerle creer, sin ninguna posibilidad de dudas, que está consiguiendo atacar la seguridad informática de la empresa. Más adelante lo veremos con más detalle.

3. Características

La característica principal de este tipo de programas es que están diseñados no solo para protegerse de un posible ataque, sino para servir de señuelo invisible al atacante, con objeto de detectar el ataque antes de que afecte a otros sistemas críticos.

Sin embargo, puede estar diseñado con múltiples objetivos, desde alertar de la existencia del ataque u obtener información sin interferir en el mismo, hasta tratar de ralentizar el ataque (*sticky honeypots*) y proteger así el resto del sistema. De esta forma se tienen *honeypots* de baja interacción, usados fundamentalmente como medida de seguridad, y *honeypots* de alta interacción, capaces de reunir mucha más información y con fines como la investigación.

Es así que, por ejemplo, la apertura de un puerto comúnmente usado para las bases de datos MySQL podría ofrecer respuestas parecidas a este sistema de gestión de bases de datos, sin tener dicho software instalado. Así es posible observar el comportamiento del atacante pudiendo finalizar en cualquier momento la conexión con cualquier excusa como *"server is shutting down"*, cuando se haya alcanzado el objetivo programado. Monitorizar un *honeypot* pasa por comprender primero cuáles son los peligros existentes y cómo funciona cada uno de ellos.

Es una advertencia que debemos aclarar, por si las dudas: los *honeypots* son herramientas que usaremos dependiendo de nuestros objetivos, no están orientados a dar soluciones. Un caso pragmático puede ser el de colocar una copia de nuestro servidor de base de datos, pero lleno de datos inventados, con el fin de realizar seguimientos.

4. Tipos de *Honeypot*

Ya existen varias alternativas que pueden ayudar a un fácil y rápido despliegue de la solución en un sistema de control. Algunos de ellos son:

- **Conpot** es un *honeypot* de sistemas de control industrial de baja interacción diseñado para ser fácil de implementar, modificar y ampliar. Al proporcionar una amplia gama de protocolos industriales comunes, permite la creación de los elementos básicos para que se pueda construir casi cualquier sistema. Actualmente se encuentra integrado dentro del Honeynet Project.

- **Gridpot** es un honeypot de código abierto que simula un SCADA de red eléctrica de forma realista. Gridpot es una combinación del *honeypot* Conpot y el simulador de redes eléctricas GridLAB-D. Esta combinación permite que este *honeypot* adquiera todas las ventajas de adquisición de datos de Conpot y un entorno de simulación con múltiples modelos que le aportan gran realismo gracias a GridLAB-D.

- **GasPot** ha sido diseñado para simular un medidor de tanque modelo Guardian AST del fabricante Veeder Root. Estos medidores son comunes en la industria petrolera para ayudar a medir el nivel de combustible. GasPot fue diseñado para ser lo más aleatorio posible para que dos instancias no sean iguales. Es de código libre y se puede descargar desde su repositorio en github.

- **iHoney** es un proyecto de investigación realizado en 2017 por el Ministerio de Industria, Energía y Turismo de España en colaboración con S2 Grupo. En este proyecto se simuló completamente una planta de tratamiento de aguas incluyendo todos los posibles elementos que podrían conformar una planta real para poder recabar la máxima información posible sobre los ataques reales que pueden recibir este tipo de instalaciones.

Desde hace años, en el mercado hay herramientas venerables que pueden servir para adentrarse en este campo. Algunas de ellas son:

- **Honeyd**: aunque es un solo *honeypot* en GNU/Linux o Windows, el atacante verá múltiples servidores panales. ¿Cuál es el truco? Honeyd crea direcciones IP virtuales, cada una con los puertos y servicios que deseemos emular. Para ayudar a comprender el concepto, imaginemos un aparato enrutador conectado por un módem a Internet y con un disco duro conectado con varias máquinas virtuales corriendo, cada una con diferentes puertos y servicios abiertos.

- **HoneyBOT**: está hecha para Microsoft Windows y tiene su interfaz gráfica integrada, lo cual la convierte en una sabia elección para todos aquellos que se inicien en el mundo de los *honeypots*. Se caracteriza por su nivel de detalle, guarda incluso todo byte recibido del atacante. Incluye interesantes gráficos que permiten ver los ataques más relevantes en un solo vistazo. Es un software privado y pertenece a "Atomic Software Solutions".

- **Specter**: es más poderoso, ya que tiene perfiles preconfigurados de varios sistemas operativos, inyecta datos codificados al atacante que permiten ser usados luego como prueba. Abre perfiles personalizados y acumulativos de cada intruso. A este programa no lo vamos a monitorizar nosotros mismos, sino que tiene informes predefinidos con datos a salvaguarda de la casa de software y desconocemos cómo los cuida porque es de código cerrado.

- **Kippo**: está escrito en Python y está alojado en GitHub con licencia libre. Se describe como un honeypot de interacción mediana, una categoría intermedia a las que describimos previamente, ya que se enfoca en SSH.

5. Ventajas e inconvenientes

Ventajas

Cada sistema de control industrial es diferente, por lo que hay que tener en cuenta que implantar un *honeypot* que simule correctamente cada sistema es una tarea difícil, aunque los beneficios de la implantación son muchos:

- Trabajan en entornos aislados.
- Debido a que utilizan servicios no legítimos producen muy pocos falsos positivos.
- Los datos son concisos y específicos de actividad no legítima.
- Distracción para los atacantes, ya que creen que están atacando un sistema real cuando en realidad no es así.
- Obtención de información sobre quién quiere dañar tu sistema de control industrial, la metodología que usa, y qué herramientas puede estar usando.
- Sirve como herramienta para testear la seguridad que posee el sistema. Si el honeypot simula fielmente la seguridad actual que posee el sistema, puede ser utilizado en un pentesting para analizar la seguridad de manera que no haya impacto alguno en el proceso industrial real.
- Puede servir para frustrar a los atacantes y disuadirles de atacar más sistemas.

Desventajas

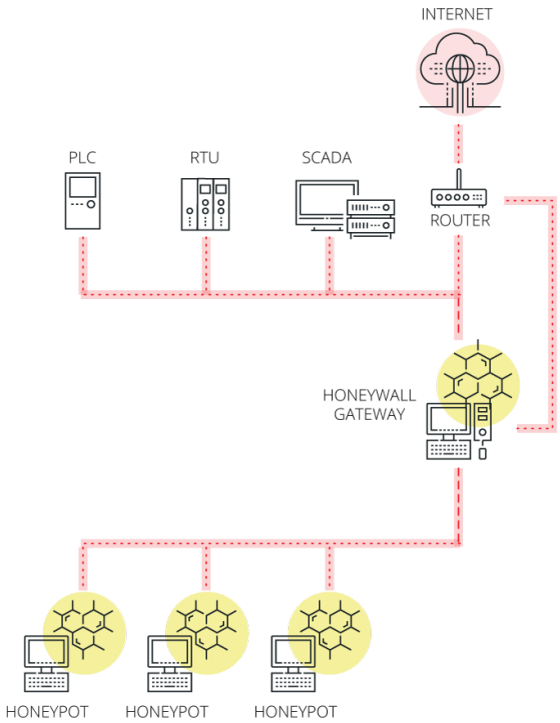
Pero hay que tener en cuenta que los *honeypots* también presentan una serie de inconvenientes a la hora de su implantación:

- Potencialmente pueden ser descubiertos por el atacante y ser usados en nuestra contra.
- Pueden ser utilizados por el atacante contra otros sistemas distintos al nuestro (ver punto anterior).
- Solo detectan ataques directos al honeypot, no detectan el entorno de la red de área local (excepto Honeyd que crea su propia red privada virtual). Sin embargo, trataremos una solución aproximada a este problema.
- Para implantar un honeypot se requieren equipos extra, con el consecuente coste, ya se trate de software y hardware real o simulado.
- La dificultad de disponer de una simulación realista de dispositivos TO es otro inconveniente, ya que, si queremos recibir un ataque, debemos de parecer lo suficiente reales para engañar al enemigo.
- Otro contrapunto es que, si de verdad se desea obtener información y aprovecharla para mejorar la seguridad, se necesita incorporar personal necesario que realice la monitorización del *honeypot* y el análisis de la información obtenida del mismo.

6. HoneyNet

Son un tipo especial de honeypots de alta interacción que actúan sobre una red entera, diseñada para ser atacada y recobrar así mucha más información sobre posibles atacantes.

Se usan equipos reales con sistemas operativos reales y corriendo aplicaciones reales. Este tipo de honeypots se usan principalmente para la investigación de nuevas técnicas de ataque y para comprobar el modus-operandi de los intrusos.



Ejemplo de HoneyNet

7. Honeyd

Características

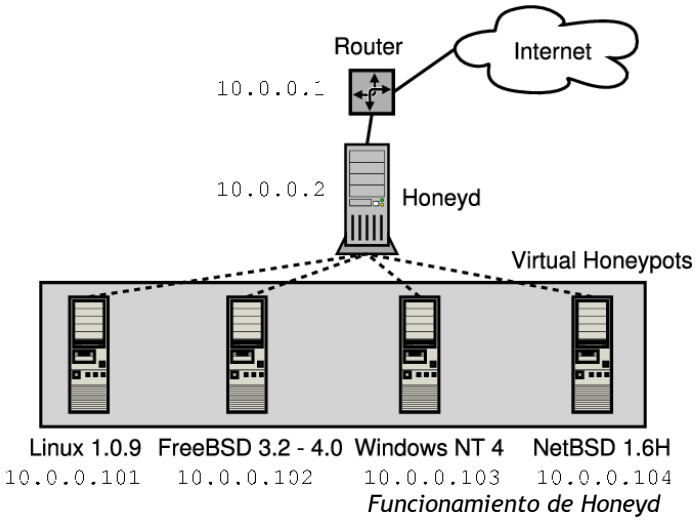
Honeyd admite una variedad de características que hacen que el demonio sea muy flexible para crear honeypots virtuales basados en host y en red. En la siguiente lista tenemos una breve descripción de las diferentes funciones que admite Honeyd:

- Simula miles de hosts virtuales al mismo tiempo.
- Configuración de servicios arbitrarios vía archivo de configuración simple:
    - Incluye proxy se conecta.
    - Toma de huellas pasivas para identificar hosts remotos.
    - Muestreo aleatorio para escalado de carga.

- Simula sistemas operativos en el nivel de pila TCP / IP:
    - Los tontos nmap y xprobe.
    - Política de reensamblaje de fragmentos ajustables.
    - Política de escaneo FIN ajustable.

- Simulación de topologías de enrutamiento arbitrario:
    - Latencia configurable y pérdida de paquetes.
    - Enrutamiento asimétrico.
    - Integración de máquinas físicas en la topología.
    - Honeyd distribuido a través de tuning GRE.

- Virtualización de subsistemas:
    - Ejecute aplicaciones UNIX reales bajo direcciones IP virtuales de Honeyd: servidores web, servidores ftp, etc.
    - Enlace dinámico de puertos en el espacio de direcciones virtuales, iniciación en segundo plano de conexiones de red, etc.



Funcionamiento de Honeyd

8. Conclusiones

Para hacernos una idea de los peligros que hay en Internet y saber que no estamos solos y sin peligro, en 2006, la BBC realizó una investigación para determinar la incidencia de ataques que podría sufrir un ordenador típico. La primera fase consistía en simplemente registrar el número y tipo de ataques, los resultados fueron que cada 15 minutos, de media, el ordenador recibía spam "molesta", normalmente ofertas fraudulentas para mejorar la seguridad del ordenador. Sin embargo, cada hora, de media, el ordenador recibía ataques más serios, de gusanos informáticos tipo SQL Slammer y MS.Blaster.

La segunda fase de la investigación consistía en dejar entrar el adware (*software no deseado diseñado para mostrar anuncios en su pantalla, normalmente en un explorador*) y spyware (*tipo de malware que los hackers utilizan para espiarle con el fin de acceder a su información personal, detalles bancarios o actividad en línea*) 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.

De ahí que los *honeypots* son una herramienta muy potente para el análisis y la defensa, también en el ámbito de los sistemas de control industrial, siempre y cuando presenten una configuración de seguridad correcta para evitar que sirvan de punto de entrada de amenazas y se tengan en cuenta todas sus ventajas e inconvenientes. Como se ha podido ver en esta documentación, ya existen varias alternativas libres de *honeypots* industriales disponibles para todo el mundo.

En definitiva, es una estrategia que puede resultar muy útil, sobre todo, en el caso de las grandes empresas, ya que suelen almacenar mucha más información confidencial y, por su propio volumen de actividad, resultan más atractivas para los posibles atacantes.

Bibliografía

https://www.pandasecurity.com/spain/mediacenter/seguridad/diferencias-sandboxing-honeypot

https://hacking-etico.com/2012/12/03/honeypot-un-tarro-de-miel-para-los-atacantes

https://www.incibe-cert.es/blog/honeypot-herramienta-conocer-al-enemigo

http://www.elladodelmal.com/2017/07/t-pot-una-colmena-de-honeypots-para.html

https://blog.pandorafms.org/es/honey-pots

https://es.wikipedia.org/wiki/Honeypot

https://www.digitalocean.com/community/tutorials/how-to-set-up-an-artillery-honeypot-on-an-ubuntu-vps

http://www.honeyd.org/general.php