**SERVIDORES WEB DE ALTAS PRESTACIONES**
GRADO EN INGENIERÍA INFORMÁTICA
UNIVERSIDAD DE GRANADA

# Honeypots

Jose Antonio Muñoz Herrera Julio José Reyes Hurtado

5 de mayo de 2019

# Índice

# 1. Introducción: Definición de Honeypot

Vivimos en la era de la digitalización. Conforme mas nos adentramos en este nuevo siglo, todo nuestro alrededor acaba tarde o temprano siendo susceptible a una traducción al mundo de los datos y estos a su vez de ser almacenados en la nube. A la par que los sistemas digitales están cada vez mas arraigados en la sociedad surge la necesidad de protegerlos de terceras partes malintencionadas. En el campo de la seguridad informática, encargada de cumplir este propósito, siempre ha tenido mas peso la parte pasiva frente a la pro-activa. Dentro de la primera podemos encontrar sistemas como los IDS (Intrusion Detection System), los firewalls, antivirus, etc... herramientas que, en resumen, evitan o al menos intentan evitar una intromisión en un sistema restringido por parte de entidades ajenas a el. Los honeypots, elemento de la seguridad del que trataremos en este documento, rompe con el rol pasivo para pasar, en mayor o menor medida, a tener un rol mas activo. El principal objetivo de estos sistemas es estudiar el comportamiento del atacante e intentar extraer información de ello a partir de un análisis sus propias acciones. Estas acciones se llevan a cabo en un entorno controlado (honeypot) donde se ofrecen una serie de acciones que simulan a las de un entorno real. Este sistema forma parte de la misma red que se quiere defender, pasando a ser un elemento mas de la misma, a priori indistinguible del resto de elementos tras un análisis superficial de la red. Desde el punto de vista de un atacante estos entornos simulados suponen un posible punto de entrada por su aparente vulnerabilidad. Una vez dentro, revelará información de forma involuntaria a través de sus acciones, explotando las distintas vulnerabilidades que el sistema ofrece. Si aceptamos como cierta esta explicación simple pero esencial del Honeypot, lo podríamos definir de la siguiente manera:

Sistema o aplicación que simula un entorno real con un repertorio de vulnerabilidades conocidas y que contiene mecanismos para almacenar las acciones que se realizan en el.

En las siguientes secciones pasaremos a hablar sobre las distintas clasificaciones entre las que se podrían englobar los distintos honeypots que existen, así como explicar un poco mas a fondo como funcionan los honeypots usando como ejemplo el producto Honeyd, una alternativa fiable de código libre dentro de las distintas opciones de los honeypots profesionales.

# 2. Configuración y despliegue

En un entorno de producción, el despliegue de los honeypots puede instalarse ya sea como entorno virtualizado o como host. La ventaja de instalarlo como entorno virtual permite un mayor control sobre la configuración del entorno, tal como el número de cores de la CPU, la memoria RAM, firewall, etc... El objetivo es configurar la máquina dentro de tu red empresarial como si fuera una máquina mas, solo que la seguridad estará desactualizada. Se pueden configurar también cuentas de acceso a varios servicios, como el correo o la administración de la red, locales a ese sistema virtualizado. Todas estas medidas persiguen el objetivo de crear un entorno lo mas realista posible pero sin comprometer demasiado la seguridad de la red en general. Este equilibrio es difícil de mantener ya que, por una parte dejar demasiadas "puertas abiertas"dentro del sistema puede derivar en acciones no controladas por parte del atacante, y por el otro un entorno demasiado restringido.

El elemento principal que nos interesa de los Honeypots es su capacidad de recopilar información tal vez vital ya sea para alertar sobre un ataque produciéndose en ese momento o que herramientas y estrategias están usándose para atacar tu red. Con este objetivo deberíamos activar los logs de toda posible acción que se pueda realizar en el sistema. Hay algunos productos profesionales que se encargan de los logs, su organización y almacenamiento, tales como SIEM. Mantener un correcto seguimiento de los logs es fundamental para hacer un correcto aprovechamiento del potencial que nos brindan los honeypots.

Existen por otra parte herramientas y sistemas ya preparados para su instalación en tu red con un mínimo de configuración. Un ejemplo es Honeyd. Esta herramienta se encarga de emular un número arbitrario de hosts dentro de una red. Cada host puede adjudicarse múltiples ips o pueden repartirse entre varios. Además proporciona distintos servicios para los hosts.

# 3. Clasificación

## 3.1. Entorno de despliegue

### 3.1.1. Cliente

Hasta ahora nos hemos referido a los Honeypots como una herramienta ubicada principalmente en la parte del servidor. Esta clasificación es en general correcta pero la misma definición de Honeypot puede aplicarse para aplicaciones en la parte del cliente. Esta clase de Honeypots se convierten voluntariamente en víctimas de un software malicioso. Se encargan de buscar activamente software malicioso o servidores que aprovechan vulnerabilidades del cliente y pasan a analizar su comportamiento. El objetivo principal de esta clase de honeypots son habitualmente los servidores web.

La estructura del cliente Honeypot puede dividirse en:

- Lista de sitios maliciosos: esta lista se puede configurar manualmente o mediante rastreo de la web, y contendrá una serie de sitios web maliciosos.
- Cliente: básicamente será el programa que se encargue de realizar las peticiones al servidor y se exponga al contagio del software malicioso. Sin embargo, un buen cliente tendrá también que tener ciertos mecanismos de contención.
- Analizador: esta parte del programa se encargará de analizar las amenazas a las que se someta el cliente y dependiendo de como se configure podrá derivar ciertas acciones dependiendo del análisis.

También en los honeypots en la parte de cliente se da una separación entre alta interacción y baja interacción. Mas adelante definiremos mas a fondo esta clasificación. Por ahora diremos que un cliente de alta interacción no tendrá a priori diferencia alguna con un cliente real, pudiendo analizar el ataque sufrido a nivel de sistema, lo que procura una mayor fuente de información pero también puede llegar a ser mas arriesgado. En cambio los que son del tipo baja interacción serán sistemas ligeros usualmente simulados.

### 3.1.2. Servidor

Todas las definiciones que hemos proporcionado en secciones anteriores deberían ya darnos una cierta idea de como funcionan los honeypots de parte del servidor. Haciendo un resumen, se trata de un servicio ubicado en un entorno virtual o físico (el servidor) que contiene vulnerabilidades a la espera de ser explotadas y posteriormente analizar la forma que han usado para hacerlo. Dentro de la clasificación del servidor podemos encontrar distintos tipos y topologías, como la Honeynet. Esta implementación se basa en una serie de Honeypots conectados entre si formando una red. Pueden llegar a compartir recursos como en una red real, dando aun mas verosimilitud desde la perspectiva del atacante. Recaban mucha mas información ya que también, a diferencia de otras posibles implementaciones, en entornos de investigación pueden llegar a usarse sistemas operativos y aplicaciones reales y no simuladas.

## 3.2. Nivel de interacción

### 3.2.1. Baja interacción

Esta clasificación es la mas usual cuando abarcamos el problema de dividir los tipos de honeypots. En la baja interacción se encuadran los sistemas que no necesitan de grandes recursos para simular un entorno real, ya sea porque la granularización del honeypot llega a nivel de proceso dentro de una computadora. Un ejemplo mencionado antes es el de Honeyd, un honeypot a nivel de daemon. Estos servicios pueden estar enfocados a diferentes recursos tales como manejo de bases de datos, gestores de correo, etc... A diferencia de los honeypots de alta interacción, los primeros suelen

ser mas susceptibles a descubrirse como honeypots, perdiendo toda su utilidad. Esto es debido a que el comportamiento suele ser mucho mas característico que uno de alta interacción, debido a la limitación de recursos de los que dispone. Esto también marca la cantidad y la calidad de información que recaba. Puede llegar a no ser del todo fiable, algo que es menos probable que pase con los de alta interacción a cambio de aumentar el riesgo implícito del uso de los honeypots.

Cabe mencionar también los honeypots de baja interacción en entorno de producción, de los que hablaremos mas adelante, los cuales en sus distintas versiones comerciales llegan a imitar partes de sistemas reales específicos usados por empresas de distinto tipo. CONPOT (ICS/SCADA Honeypot) esta especialmente diseñado para desplegarse en industrias que trabajan con control automatizado.

#### 3.2.2. Alta interacción

A este nivel, si con el anterior hablábamos de aplicaciones de poca complejidad que podían no llegar a proporcionar información del todo fiable o que su estatus secreto como honeypot podía verse comprometido debido a lo reducido de sus posibilidades, ahora nos encontramos en el caso contrario. Sistemas reales con complejas configuraciones de firewall y red, intentando equilibrar la cantidad de información su calidad por un lado, y por el otro el no permitir demasiada libertad que pudiera inducir a escapes no controlados. Debido a su costosa implementación y soporte, en un ambiente empresarial su instalación puede resultar demasiado arriesgado. Antes nos referíamos a escapes no controlados por parte de terceros maliciosos que pudieran escapar del entorno del honeypot. El hecho de que los sistemas sean reales con verdaderas vulnerabilidades, el honeypot puede ser comprometido completamente. A cambio, la cantidad de información, la posibilidad de estudiar el comportamiento de la infección, permite usarse para analizar y en respuesta poder encontrar una forma de neutralizar amenazas como vulnerabilidades Zero-Day.

### 3.3. Propósito

#### 3.3.1. Entorno de producción

Los honeypots en entorno de producción persiguen emular partes de un sistema de producción real, ofreciéndose como cebo frente a ataques para retrasar y dejar mas tiempo de reacción para reaccionar. Ayuda por una parte a proteger los verdaderos puntos críticos del sistema y por la otra a conocer la manera en la que se esta atacando. Partes del sistema que intentan emular suelen ser principalmente servicios, como bases de datos, invitando a la vulneración de este sistema. También pueden incluso emular backdoors o virus instalados dentro de la propia red de los que puedan aprovecharse terceros. La ventaja de este tipo de honeypots es su facilidad de instalación y mantenimiento.

#### 3.3.2. Entorno de investigación

Al contrario que los anteriores los honeypots orientados al a investigación no persiguen proteger específicamente una organización sino que pretenden dar recopilar información sobre la comunidad de blackhats. Quieren encontrar las fallas que las organizaciones pueden tener junto como saber como pueden ser atacadas, con que herramientas y como han conseguido esas herramientas. Ayudan a la comunidad de seguridad tanto gobierno como empresas. Por ello normalmente este tipo de honeypot serán de alta interacción ya que para recabar el máximo de información posible necesitan simular sistemas completos.

Las diferencias entre los honeypots de producción y de investigación no son absolutas ya que pueden usarse con propósitos similares.

## 4. Ventajas y desventajas de su aplicación

Como hemos visto los honeypots son una herramienta de mucha utilidad, dándonos información

de utilidad con respecto a posibles atacantes a nuestra red o a nuestra empresa. A continuación vamos a presentar las ventajas e inconvenientes que podrían acarrear el uso de uno o varios honeypots (honeynets) para proteger tu red.

## 4.1. Ventajas

## 4.2. Datos aportados

En la era de la información una de las cosas mas valiosas por no decir la que más son los datos, que nos aportan información sobre cualquier tema sobre el que deseemos trabajar, y los honeypots no son una excepción. En las empresas y organizaciones las herramientas utilizadas para coger información sobre posibles atacantes como los IDS o los firewalls puede ser tan grande que es posible que los datos específicos que estamos buscando sera muy difícil de clarificar o de clasificar recogiendo gigabytes de datos, logs, etc... En este campo los honeypots son clave ya que en ellos se recoge información fácil de entender y posibilita un análisis ágil y sencillo, recogiendo pocos megas a lo largo de un día pudiendo así detectar comportamientos sospechosos más fácilmente.

### 4.2.1. Gasto de recursos

En ocasiones las herramientas comunes de detección de intrusos o los firewalls pueden llegar a un punto en el que no pueden seguir cumpliendo con sus funciones debido a la sobrecarga sobre ellos lo que puede generar la pérdida de datos y paquetes.

Los honeypots no tienen este problema ya que capturan y tratan con información específica por lo que no llegarán a colapsar al contrario que IDS que soportan una alta carga de tráfico en toda la red del sistema. Con los honeypots no es necesario realizar un gran gasto en hardware ni en software ya que no precisan del uso de una gran cantidad procesador o RAM, pudiéndose usar ordenadores o PC's antiguos que no estén siendo utilizados y configurar el honeypot en ellos.

### 4.2.2. Simplicidad

Una de las grandes ventajas de los honeypots puede ser su sencillez a la hora de configurarlos. No requieren de complejos algoritmos ni desarrollo sino que simplemente necesitamos desplegarlo en el punto de la red que queramos analizar dejarlo en marcha y esperar resultados, aunque también existen honeypots que pueden ser más complejos como por ejemplo los que se utilizan para investigación, aunque todos se basan en una premisa básica que es, si alguien se conecta comprueba que ha hecho. Gracias a esta simplicidad se pueden evitar fallos o posibles entradas a la red ya que cuanto más complejo es un sistema se pueden encontrar mas fallas en el.

### 4.2.3. Confianza

Cuando los firewall, IDS y otras herramientas que se utilizan para evitar que agentes externos penetren en nuestra red realizan su trabajo es posible que la empresa u organización se pregunte: ¿Porque tener estos dispositivos tan costosos cuando no hemos sido atacados en tres años?. Esto se debe a que como se ha dicho anteriormente las herramientas antes mencionadas dan una capa de protección que a la red que puede evitar la intrusión de alguien ajeno a la red.

Para este caso los honeypots nos puede esclarecer la realidad en la que vivimos y enseñar que las herramientas que se han utilizado no han sido en vano sino que han estado parando ataques externos durante todo este tiempo, ya que al dejar una vía abierta para entrar se puede demostrar lo que en realidad se encuentra fuera de la red y el valor que tienen las herramientas que no permiten que se lleven a cabo ese tipo de ataques que se han hecho al honeypot.

## 4.3. Desventajas

Con todas estas ventajas explicadas podríamos decir que los honeypots son el arma definitiva para defenderse contra ataques externos, nada más lejos de la verdad. Por ello que los honeypots no sean los sistemas principales de defensa sino que son un apoyo para estos.

### 4.3.1. Campo de acción

Con los honeypots podemos controlar lo que ocurre únicamente en el honeypot, a diferencia de otras herramientas que controlan la red entera. Si alguien no deseado entrara en nuestra red no seria para nosotros posible ver lo que esta pasando. Pueden enviar información muy concisa y específica pero no le será posible ver que ocurre a su alrededor.

### 4.3.2. Fingerprinting

Otra desventaja en esta herramienta es que los atacantes identifiquen el sistema como honeypot mediante un comportamiento o características específicas. Por ejemplo si estuviéramos emulando en nuestro honeypot cuando el servidor hace una respuesta, algunos honeypots tienen por ejemplo el comando de HTML lenght como legnth, este error puede identificar rápidamente al honeypot. O error frecuente es simular un servidor con un sistema operativo y que presente características de otro sistema operativo.

Este tipo de vulnerabilidades son especialmente dañinas para los honeypots de investigación ya que da la libertad a los intrusos de proporcionar información que lleve al falseo de datos recogidos.

### 4.3.3. Riesgo

Los honeypots pueden introducir cierto riesgo al entorno ya que, una vez atacados podrían llegar a pivotar hasta dentro de la red.

Como se ha visto anteriormente en los tipos de honeypots que podemos ver, distinguimos entre los de baja, media y alta interacción dependiendo del número de servicios que emulen. Cuantos más servicios sean emulados habrá más flancos para que se pueda romper la jaula del honeypot y lanzar ataques a la red interna.

Debidos a estos inconvenientes los honeypots no pueden remplazar a los demás sistemas de seguridad pero añaden un valor en los mecanismos de securización de las redes que pueden ser vitales en un momento dado.

# 5. Referencias

Honeypots: Tracking Hackers. Lanze Spitzner (2002). http://www.it-docs.net/ddata/792.pdf
Production Honeypots: An Organization's view. Abhilash Verma (2003)https://www.giac.org/paper/gsec/3585/production-honeypots-organizations-view/105831
The honeynet projects. https://www.honeynet.org/
Taxonomy of Honeypots. Christian Seifert, Ian Welch, Peter Komisarczuk (2012) http://www.mcs.vuw.ac.nz/comp/Publications/CS-TR-06-12.abs.html