ugr | Universidad de Granada

SERVIDORES WEB DE ALTAS PRESTACIONES

HoneyPots

Trabajo realizado por:

- Javier Garrido Montes
- Ignacio Irurita Contreras

1. Introducción

En seguridad toda medida es poca y hay que estar innovando continuamente (actualizando políticas y medios para afinar los recursos de seguridad) para no dejar huecos por donde puedan colarse los intrusos, pero como esto no siempre es evitable (la seguridad absoluta en la práctica no existe, podemos siempre irnos aproximando a ella, pero como concepto constituye un objetivo irrealizable), es como de manera obligada o natural se abre paso a todo un universo de técnicas más elaboradas e incluso ingeniosas, como es facilitar la entrada a la red pero por caminos falsos que no conducen a nada concreto o esperable para un posible atacante y que permiten al responsable de la seguridad del sistema detectar los intentos de intrusión, con lo que se está sobre aviso y es más fácil protegerse.

2. HoneyPots

Un Honeypot es un sistema diseñado para analizar cómo los intrusos emplean sus armas para intentar entrar en un sistema (analizan las vulnerabilidades) y alterar, copiar o destruir sus datos o la totalidad de éstos (por ejemplo borrando el disco duro del servidor).

Los primeros conceptos fueron introducidos por primera vez por varios íconos en la seguridad informática, especialmente aquellos definidos por Cliff Stoll y Bill Cheswick. Desde entonces, han estado en una continua evolución, desarrollándose de manera acelerada y convirtiéndose en una poderosa herramienta de seguridad hoy en día.

Un honeypot puede ser tan simple como un ordenador que ejecuta un programa, que analiza el tráfico que entra y sale de un ordenador hacia Internet, “escuchando” en cualquier número de puertos. El procedimiento consiste en mantener una debilidad o vulnerabilidad en un programa, en el sistema operativo, en el protocolo, o en cualquier otro elemento del equipo susceptible de ser atacado, que motive al atacante a usarlo, de manera que se muestre dispuesto a emplear todas sus habilidades para explotar dicha debilidad y obtener acceso al sistema.

Por otro lado, un honeypot puede ser tan complejo como una completa red de ordenadores completamente funcionales, funcionando bajo distintos sistemas operativos y ofreciendo gran cantidad de servicios. Cuando algún sistema que está incluido en dicha red sea atacado de alguna forma, se advierte al administrador.

Otra opción muy utilizada es crear honeypots completamente virtuales: programas específicamente diseñados para simular una red, engañar al atacante con direcciones falsas, IP fingidas y ordenadores inexistentes, con el único fin de confundirlo o alimentar el ataque para analizar nuevos métodos. Si algo tienen en común los honeypots es que no guardan ninguna información relevante, y si lo parece, si se muestran contraseñas o datos de usuario, son completamente ficticios.

3. Clasificación de los HoneyPots

La mejor manera de diferenciar estos tipos de aplicaciones es por la interactividad. Es decir, hasta qué nivel deja interactuar al atacante con el Honeypot. Entonces clasificamos, según este factor por:

Baja interacción

Suelen ser creados y gestionados por organizaciones dedicadas a la investigación del fraude en Internet, o cualquier tipo de organización que necesite investigar sobre las nuevas amenazas en la red.

Se suelen tratar de sistemas específicos que emulan servicios, redes, pilas TCP o cualquier otro aspecto de un sistema real, pero sin serlo. Simulan ser un servicio, y ofrecen respuesta a un subconjunto de respuestas simple. Por ejemplo, un honeypot que simule ser un servidor de correo, puede simular aceptar conexiones y permitir que se escriba en ellas un correo, aunque nunca llegará a enviarlo realmente.

Son muy complejos de administrar y mantener, y la información que reciben debe ser lo más extensa posible, ésta debe ser organizada y analizada para que sea de utilidad.

Normalmente este tipo de honeypots no está destinado a “atrapar” atacantes reales, sino herramientas automatizadas.

Este tipo de honeypots, tienen el problema de que en ellos resulta más complejo descubrir nuevos tipos de ataques. Están preparados para simular ciertos servicios que se saben atacados, y a responder de cierta manera para que el ataque crea que ha conseguido su objetivo. Pero en ningún caso puede comportarse de formas para las que no está programado, por ejemplo para simular la explotación de nuevos tipos de amenazas.

Alta interacción

Suelen ser usados por las compañías en sus redes internas. Estos honeypots están construidos con máquinas reales. Se colocan en la red interna en producción. Si están bien configurados, cualquier intento de acceso a ellos debe suponer una alerta a tener en cuenta. Puesto que no tienen ninguna utilidad más que la de ser atacados, el hecho de que de alguna forma se intente acceder a ese recurso significa por definición que algo no va bien.

Cada interacción con ese honeypot se considera sospechosa por definición. Todo este tráfico debe ser monitorizado y almacenado en una zona segura de la red, y a la que un potencial atacante no tenga acceso. Esto es así porque, si se tratase de un ataque real, el intruso podría a su vez borrar todo el tráfico generado por él mismo, las señales que ha ido dejando, con lo que el ataque pasaría desapercibido y el honeypot no tendría utilidad real.

Las ventajas que ofrecen los honeypots de alta interacción es que pueden prevenir ataques de todo tipo. Tanto los conocidos como los desconocidos. Al tratarse de un sistema real, contiene todos los fallos de software conocidos y desconocidos que pueda albergar cualquier otro sistema.

Comparación de principales características

Baja Interacción	Alta Interacción
Emulan servicios, vulnerabilidades, etc.	Servicios reales, sistemas operativos o aplicaciones
El riesgo que corren es menor	El riesgo que corren es mayor
Capturan menos información, pero más valiosa	Capturan mucha información. Dependen de su sistema de clasificación y análisis para evaluarlo.

4. Diseñando y construyendo un HoneyPot

Actualmente existen multitud de herramientas libres que pueden ayudar en el despliegue de honeypots para este tipo de investigaciones o incluso, teniendo los conocimientos necesarios, desarrollar software personalizado. Algunas de estas herramientas se usan desde consola de comandos, siendo necesario analizar e interpretar los logs que generan para saber que está ocurriendo, otras poseen un entorno gráfico desde donde poder visualizar los datos obtenidos.

Para dar un paso más en la investigación, se pueden utilizar:

- Sistemas de identificación de intrusos (IDS) a fin de determinar qué ataque se está realizando, siempre que exista una firma del IDS que lo identifique.
- Cortafuegos de aplicación web, WAF (del inglés Web Application Firewall) en servidores web para determinar e identificar ataques contra servicios web.
- Listas de reputación (públicas y privadas) para contrastar las IP atacantes contra listas reconocidas por otras entidades
- Motores antivirus para realizar el análisis de las muestras obtenidas.
- Realización análisis estático y dinámico de muestras depositadas en los honeypots
- Correlación de eventos.

Ejemplo de Herramienta

Honeystation, honeypot desarrollada en INCIBE.

Gracias a este tipo de sistema y a través de una implementación desarrollada en INCIBE, en los últimos meses se han detectado diversos tipos de ataques que han sido notificados a sus principales interesados.

Entre estos ataques destacamos:

- Ataques de denegación de servicio usando Ips falsificadas (spoofing) pertenecientes a un proveedor americano contra diversos servicios web.
- Uso de servicios de un importante ASN extranjero, para realizar ataques SSH para comprometer servidores vulnerables y utilizarlos como proxy para obtener beneficios a través de pago por click.

Información recopilada con Honeystation

Mediante el uso de HONEYSTATION, se obtiene información en tiempo real sobre:

- Origen del ataque
- Nombre del ASN
- Dirección IP del Atacante
- Puerto Atacado
- Número de intentos de ataque
- Chequeo contra listas de reputación públicas y privadas.
- Chequeo contra listas de reputación generadas por los propios honeypots.
- Chequeo contra sistemas de identificación de intrusos
- Chequeo contra WAF
- Tendencias de ataques

Monitorización

No solo se monitorizan los puertos clásicos como 21,22, 23,445, 3389 0 5900, sino que se monitoriza todo el rango de puertos TCP/UDP con objeto de identificar los puertos/ servicios atractivos para los atacantes y estudiar las acciones realizadas en ese puerto.

Por otra parte, mediante correlación de eventos se obtiene valor de toda la información obtenida por los honeypots y la que ya disponemos en nuestros sistemas, permitiendo la generación de alertas a los departamentos encargados de gestionarlas.

Visualización de resultados

HONEYSTATION permite 3 tipos de vistas:

- **Vista Estado del Honeypot:** Muestra una visión del estado actual de la Honey desplegada de forma jerarquizada (Pais - ASN - IP - Puerto - Honey). El sistema permite filtrar por cualquiera de los campos y mostrar solo aquella información por la que estamos interesados. Permite visualizar rankings de países, puertos y ASN atacantes así como visualizar los atacantes potenciales y, en el caso de disponer de información suficiente, el tipo de ataque realizado o como la clasificación de la dirección IP atacante al cotejarse con la información disponible

- **Vista Geolocalización por país y nivel de ataque:** Muestra el origen de los ataques hacia la Honey, informando del número de ataques registrados y la intensidad del ataque desde un determinado país. También da una visión simplificada de la vista Estado del Honeypot

- **Vista Geolocalización precisa:** Permite determinar de una forma más precisa la geolocalización del atacante, normalmente a nivel de comunidad, provincia o ciudad.

5. Donde poner un HoneyPot

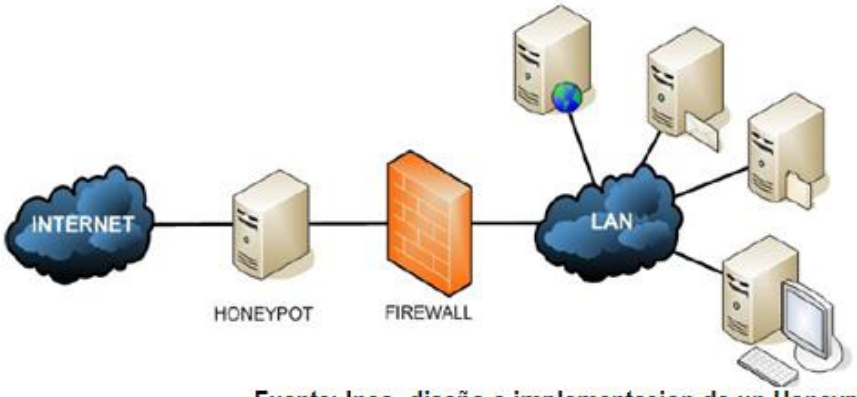
En las instituciones y las universidades los investigadores especializados en Honeypot han identificado tres zonas referentes para implementar los sistemas trampa.

1. Delante el Firewall

Al colocarlo delante del Firewall, hace que la seguridad de nuestra red interna no se vea comprometida en ningún momento ya que nuestro Firewall evitara que el ataque vaya a nuestra red interna.

Las dificultades al usar este método son:

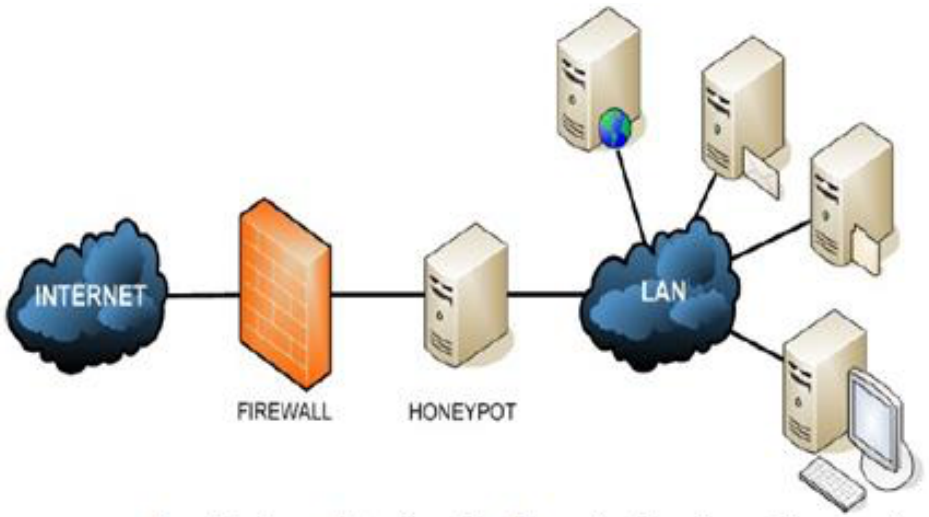
- El ancho de banda que se consumiría, ya que al estar en el exterior del Firewall no abra dificultad en acceder a él.
- A él estar fuera de nuestro Firewall, no podremos controlar los ataques internos.



Fuente: Inco, diseño e implementacion de un Honeypot

2. Detrás del Firewall

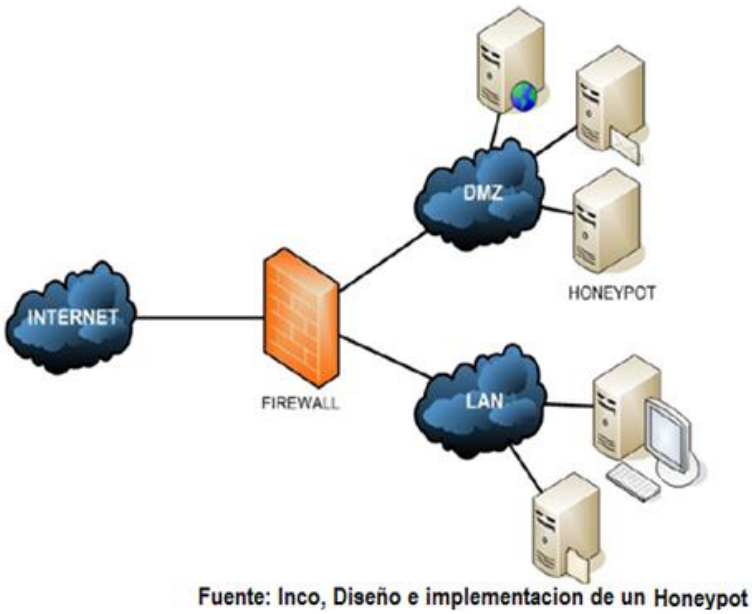
Esta opción nos permite el control de los ataques internos y externos de cualquier tipo, el principal problema que presenta este método es que requiere una configuración específica para dejar el acceso al Honeypot pero no a nuestra red. Lo cual provoca posibles fallos de seguridad en la filtración de tráfico.



Fuente: Inco, Diseño e implementacion de un Honeypot

3. En una zona desmilitarizada

Al posicionarlo aquí se hace posible la separación del Honeypot de la red interna y la unión con los servidores, esta posibilidad nos permite detectar tanto ataques internos como externos con una pequeña modificación del Firewall.



Fuente: Inco, Diseño e implementacion de un Honeypot