HONEYPOTS

CFTIC

17 de Mayo de 2023

ESTUDIANDO AL ATACANTE

HONEYPOTS - CONTENIDOS

- Introducción
- ¿Qué es un honeypot?
- Tipos de honeypot y objetivos.
- Honeynet.
- Proyectos software honeypot opensource.
- Mejores prácticas en la implantación de honeypots.
- Taller: Implantación de un honeypot y simulación de un ataque. Análisis de los resultados.

PONENTE

Ponente: ***Nacho Barnés***

Tras dedicarse a la técnica de sistemas durante 15 años, se vuelca con la ciberseguridad los últimos 7.
Especializado en DFIR y en general en seguridad defensiva, fruto de la experiencia anterior y de la actividad de respuesta ante incidentes.
En posesión de las certificaciones EC-Council CHFI y CEH Master e IRCP de Securizame, instructor del EC Council y autor de cursos sobre forensia y respuesta ante incidentes.

INTRODUCCIÓN

¿Quién ataca nuestros sistemas?

Es importante entender el escenario en el que estamos, el cibercrimen es una industria:

El negocio del cibercrimen se estima en unos 1.500.000 millones de euros. (13th GDP)

El costo global de los incidentes de ciberdelincuencia aumentó de $ 3.000 millones a principios de 2015 a $ 6.000 millones en 2022.

INTRODUCCIÓN

CIBERSEGURIDAD

El 60% de las empresas que sufren un ciberataque se ven obligadas a cerrar

EE.UU. declara estado de emergencia tras un ciberataque a la mayor red de oleoductos del país

Redacción
BBC News Mundo

Tecnología y Sociedad

Una persona fallece a causa de un ciberataque por primera vez en la historia

Una paciente que necesitaba cuidados intensivos tuvo que ser trasladada cuando los sistemas del hospital en el que se encontraba dejaron de funcionar por un ataque ransomware. La policía alemana atribuye su muerte a los piratas informáticos

Tres semanas KO por un ciberataque: así tienen secuestrados los sistemas de Adeslas

La compañía de salud, una de las más grandes de España, lleva desde el 11 de septiembre sin poder operar con normalidad debido a un potente ataque 'ransomware'

Así es el ciberataque que mantiene totalmente paralizada a Garmin

Los 'hackers' piden 8,5 millones de euros por detener el secuestro de datos que afecta desde el jueves a la plataforma de control del ejercicio y posicionamiento por GPS

INTRODUCCIÓN

Actores involucrados

- ✓ **Ciberdelincuentes**: Cometen delitos comunes apoyados en los sistemas digitales y redes.
- ✓ **Hacktivistas**: Realizan acciones reivindicativas en el ciberespacio.
- ✓ **Ciberterroristas**: Utilizan el ciberespacio para cometer actos de terrorismo.
- ✓ **Estados**: Realizan acciones ofensivas en el ciberespacio para ganar ventaja geoestratégica.

Revisar informe https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6786-ccn-cert-ia-24-22-ciberamenazas-y-tendencias-edicion-2022-1/file.html

INTRODUCCIÓN

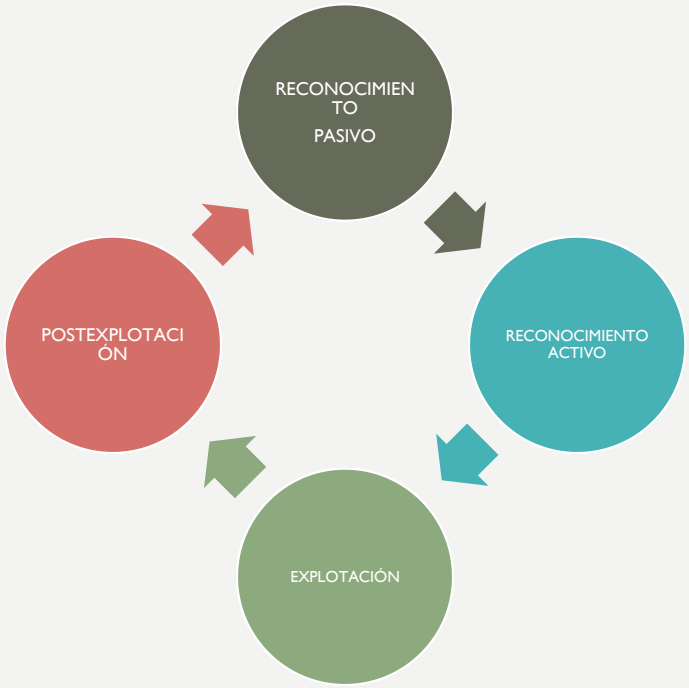
Tipos de ataques, en cuanto a selección de la víctima

- ✓ **Dirigidos**: Ataques que tienen un objetivo concreto, como en el caso de las auditorías de seguridad, las APT's u otros ataques con un objetivo definido a priori.

- ✓ **No Dirigidos**: Ataques que buscan sistemas que puedan ser comprometidos, con múltiples fines:
  - ✓ Usar recursos para realizar ataques DDoS u otras campañas, spam, clicks, etc…
  - ✓ Cifrar la información que contienen y pedir un rescate, caso del Ransomware.
  - ✓ Usarlo para compartir recursos ilegales, como pornografía infantil u hospedar un sitio de Phishing.
  - ✓ Usar los recursos computacionales para el minado de criptomonedas.
  - ✓ ¿O porqué no, para todos ellos?

INTRODUCCIÓN

Metodología y técnicas. TTP's



Metodología de hacking:

- ✓ Reconocimiento pasivo: Búsqueda de información sin "tocar" la víctima. Esencial en ataques dirigidos.
- ✓ Reconocimiento activo: Escaneo de puertos, enumeración de servicios, usuarios. Todo interactuando con el sistema objetivo. Esencial en todo ataque.
- ✓ Explotación: Obtención de la primera conexión a los sistemas de la víctima.
- ✓ Postexplotación: EoP, pivoting, uso de los sistemas para los objetivos descritos, medidas antiforenses.

Revisar https://attack.mitre.org/ y https://attack.mitre.org/groups/G0007/

INTRODUCCIÓN

Inteligencia, la información útil.

"El término información debe diferenciarse del de inteligencia. **Información** equivale a noticia de un hecho en su sentido más amplio. El concepto información debe entenderse, por tanto, como el elemento de partida para la elaboración de **inteligencia**, considerada ésta como el resultado de valorar, analizar, integrar e interpretar la información".

¿QUÉ ES UN HONEYPOT?

Se trata de un sistema informático trampa o señuelo, (Deception) expuesto con atractivos para el atacante de forma que resulta atacado antes que cualquier otro sistema de la organización.

Los objetivos principales son dos:

1. Detectar intrusiones en la organización, monitorizando el Honeypot, antes de que lleguen a sistemas reales.
2. Investigar sobre las técnicas utilizadas por los atacantes como fuente de inteligencia y TTP's.

¿QUÉ ES UN HONEYPOT?

Atractivos para el atacante:

- Exponer vulnerabilidades conocidas y fáciles de atacar.

  Es una estrategia habitual, válida para atraer los sistemas automáticos y a los atacantes no altamente cualificados. No válido para actores estado, por ejemplo. Muy adecuada para la obtención de inteligencia.

- Simular un sistema de alto interés, por su información, actividad y protección.

  Al contrario de lo anterior, busca simular un sistema lo más real posible, reduciendo la desconfianza del atacante de estar ante un señuelo.

- Exponer muchos servicios, incluso una red con múltiples dispositivos y servicios, Honeynet.

  Invita al atacante a realizar múltiples tareas de escaneo y enumeración de servicios, lo que incrementa la obtención de información para generar inteligencia.

TIPOS DE HONEYPOT

En función de las capacidades de interacción:

- Baja interacción.

  Honeypots que exponen un número reducido de servicios, incluso uno sólo. Pueden ser sistemas dedicados a la función de detección de intrusión, ya que no ofrecen excesiva información en cuanto a inteligencia. Se llegan incluso a incluir datos ficticios que permiten realizar un seguimiento. El atacante puede tener la sensación de estar frente a un sistema real de producción.

- Alta interacción .

  Al contrario que los anteriores, busca que el atacante o los atacantes pongan de manifiesto todas sus habilidades para vulnerar distintos servicios y por tanto, ser una fuente de inteligencia muy jugosa. Para ello, exponen múltiples servicios y capacidades de interacción con estos, como ejecución de shellcodes, comandos, exploits, etc…

TIPOS DE HONEYPOT

En función de la finalidad:

- Producción

  El fin principal es detectar de forma prematura un ataque así como retrasar el alcance de los sistemas críticos. Adicionalmente nos vale para recopilar información básica de IP's, geolocalización y fecha y hora.

- Investigación

  Lo se que busca es exponer un conjunto de sistemas lo suficientemente complejo como para que el adversario utilice distintas técnicas y le permita evolucionar en sus intrusiones. Es habitual la simulación de un conjunto de equipos conectados en red, lo que da lugar al concepto de Honeynet.

TIPOS DE HONEYPOT

En función del servicio suplantado:

- Base de datos, ofreciendo un conjunto de datos señuelo.
- Malware, permitiendo capturar muestras y comportamientos de estas muestras usadas para vulnerar servicios.
- WEB, para el análisis de técnicas de explotación de entornos WEB.
- De servicios específicos, SMB, FTP, SSH, MySQL, …
- De sistemas industriales, simulando sistemas ICS como SCADA.
- Específicos para un determinado malware o botnet.
- Detección de arañas o crawler, que inyectan código en los recopiladores de información que puede ser seguido posteriormente.

PROYECTOS HONEYPOT OPENSOURCE

Algunos ejemplos…

- Artillery

Honeypot multiplataforma, escrito en Python. Expone varios puertos y monitoriza las IP's que se conectan, incluyéndolas en un fichero de "banned" IP. Notifica cuando se recibe una conexión. Válido como detector de intrusiones.

- Kippo

Escrito también en Python, es un honeypot de interacción media, focalizado principalmente en SSH. Permite ofrecer al atacante una Shell y un sistema de ficheros ficticio contra el que actuar, registrando toda la actividad tanto de intentos de conexión como de ejecución de comandos si se consigue establecer una sesión.

PROYECTOS HONEYPOT OPENSOURCE

Algunos ejemplos…

- Elasticpot

Se trata de un Honeypot específico para similar un Elasticsearch abierto a Internet.

- Dionaea

Honeypot que levanta varios servicios comunes, entre ellos HTTP, FTP, TFTP, SMB y loguea con herramientas habituales, como fail2ban, hpfeeds, log_json, log_sqlit. Permite emular un entorno x86 para ejecutar shellcode para Windows. Su función principal es la captura de Malware.

- Honeytrap

Es un sistema para ejecutar, monitorizar y gestionar otros honeypots, escrito en Go. De esta manera podemos agregar otros honeypots, gestionarlos y analizar la información obtenida de forma conjunta, creando honeypots de alta interacción.

Revisar la web: https://github.com/paralax/awesome-honeypots

MEJORES PRÁCTICAS IMPLANTACIÓN

- ✓ Tener claro el objetivo perseguido.
- ✓ Conocer la herramienta que vamos a exponer, así como los datos que nos ofrece.
- ✓ Asegurar el aislamiento. Los contenedores son una herramienta fantástica para el despliegue de honeypots, pero su nivel de aislamiento no está al nivel de una máquina virtual. Es importante tener claro a qué puede dar lugar el compromiso de nuestro honeypot.
- ✓ Antes de exponer el señuelo, tener claro el procedimiento de actuación. No será lo mismo si lo uso para obtener información o si lo uso para detectar un ataque.
- ✓ Dado que no deja de ser un sistema más de nuestra red, incluirlo en los planes de monitorización y actualizaciones.
- ✓ Los honeypot también se pueden usar para detectar ataques internos.

IMPLANTACIÓN DE UN HONEYPOT

Criterios de selección

Para este taller hemos buscado una solución Honeypot que permita:

- ✓ Alta interacción
- ✓ Visualización avanzada de datos
- ✓ Simplicidad de instalación
- ✓ Probar distintas soluciones de Honeypot, en forma agregada
- ✓ Que nos permita instalarlo en un entorno de virtualización nivel 2 como Virtual Box
- ✓ Que disponga de buena documentación
- ✓ Que permita simular los servicios más habituales

https://github.com/telekom-security/tpotce

IMPLANTACIÓN DE UN HONEYPOT

T-POT Servicios

Ofrece cinco grupos de servicios

- ✓ Servicios del propio OS (Debian 11)
  - *SSH y Cockpit para gestión web remota.*
- ✓ ELK Stack
  - *Para el almacenamiento, búsqueda y presentación de logs.*
- ✓ Herramientas
  - *ElasticVUE*, GeoIP Attack Map, Spiderfoot y Ciberchef.
- ✓ Honeypots en forma de imágenes Docker.
  - *22 honeypots de los que se instancian contendores para su puesta en marcha.*
- ✓ Herramientas de Network Security Monitor
  - *Que permiten analizar el tráfico capturado en busca de las distintas trazas e indicadores de los ataques.*

IMPLANTACIÓN DE UN HONEYPOT

T-POT Requisitos

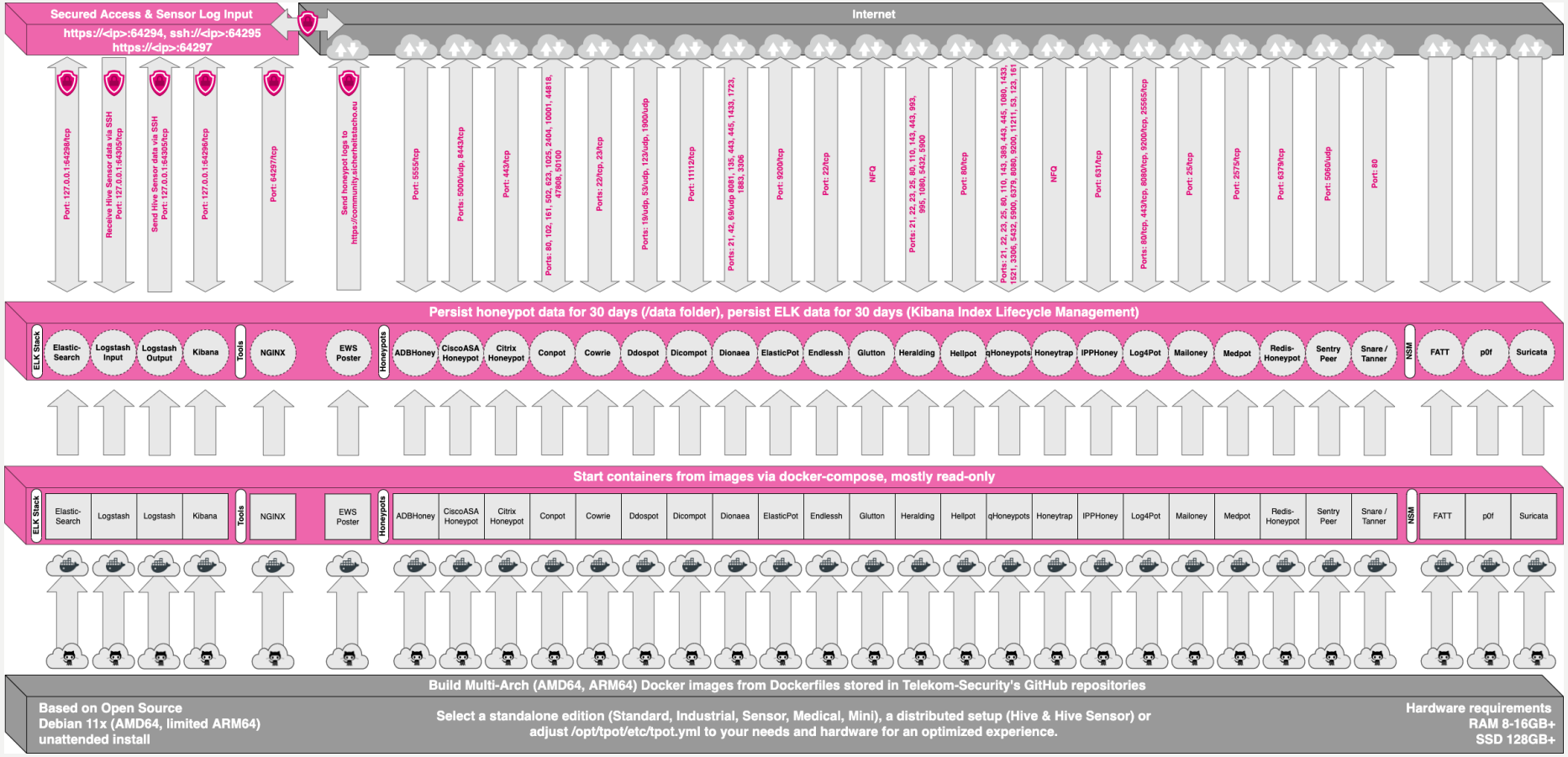
Dispone de distintos modos de instalación.
La instalación estándar, que es la que vamos a utilizar que permite usar todos los servicios, requiere:

- ✓ *Mínimo 8 GB RAM y 128 GB Disco*
- ✓ *IP asignada por DHCP.*
- ✓ *Salida directa a Internet, sin proxy.*
- ✓ *Redirección de los puertos entrantes en los que queremos exponer servicios Honeypot.*
- ✓ *Estos requisitos son para su funcionamiento sin mayor configuración.*
- ✓ *Recomendable limitar el acceso a los puertos >64000 por ser de gestión del propio t-Pot.*

Relación de puertos necesarios: https://github.com/telekom-security/tpotce/#technical-concept

IMPLANTACIÓN DE UN HONEYPOT

Arquitectura de T-Pot



IMPLANTACIÓN DE UN HONEYPOT

Herramientas externas

Además del conjunto de Honeypots, T-Pot ofrece integradas algunas herramientas adicionales:

- Spiderfoot: Herrmienta de OSINT que podemos utilizar para recopilar información sobre IP's y dominios encontrados en los orígenes de los ataques.

- Cyberchef: Interesnate proyecto que integra múltiples utilidades de criptografía, cáculo de hashes, CRC's, etc…

- SecurityMeter: Proyecto que centraliza los datos de los distintos T-POT en una consola central en la que se pueden visualizar todos los ataques de forma simultánea.

DEMO TIME

- ✓¿Qué pasa cuando publico un servicio conocido en Internet?
- ✓¿De dónde provienen las amenazas?
- ✓¿Qué técnicas se usan para atacar mis sistemas?
- ✓¿Que binarios debo buscar? ¿Y comandos?
- ✓Como pentester, ¿Qué encuentro si escaneo un T-Pot?
- ✓….

DEMO TIME – INSTALACIÓN Y VISUALIZACIÓN DE DATOS EN T-POT.

CONCLUSIONES

Estudiar al atacante mejora nuestra psotura de seguridad:

- **Muchas Ip’s maliciosas ya figuran reportadas.**
- **Los puertos estándar nos los van a localizar de inmediato. La seguridad por oscuridad puede ser un refuerzo allá dónde se pueda permitir.**
- **Cuánto más personalicemos nuestro honeypot, más útil para prevenir ataques a nuestra infraestructura.**
- **Subimos el nivel de exigencia al atacante, lo que redunda en un menor número de posibles actores maliciosos.**
- **…**

¡Muchas gracias por vuestra atención!