Que es T-Pot?

T-Pot es una potente herramienta de **HoneyPots todo en uno**, de código abierto la cual esta **desarrollada por Deutsche Telekom**. Esta plataforma multiusos **integra**
más de 20 HoneyPots diferentes, junto con numerosas opciones de visualización y herramientas de seguridad, lo que la convierte en una solución completa para la detección y prevención de amenazas cibernéticas.

A través de la implementación estratégica de T-Pot y el análisis detallado de los datos recopilados, en los que se buscará:

1. Identificar amenazas no detectadas por sistemas convencionales.
2. Comprender las tácticas, técnicas y procedimientos (TTP) de los atacantes.
3. Evaluar la efectividad de las defensas existentes.
4. Mejorar las capacidades de respuesta ante incidentes de seguridad

Requisitos previos

RAM

32GB para evitar posibles fallos por falta de recursos. Aunque T-Pot puede funcionar con menos memoria, esta cantidad asegura un rendimiento óptimo y la capacidad de ejecutar todos los HoneyPots sin problemas.

Almacenamiento

300GB de espacio en disco. Este amplio espacio de almacenamiento permite capturar y almacenar una gran cantidad de datos de ataques sin riesgo de quedarse sin espacio rápidamente.

Sistema operativo base

Debian 12. T-Pot esta diseñado para funcionar sobre Debian, y la versión 12 es la más reciente compatible con la plataforma.

Entorno controlado

Se recomienda el uso de una red totalmente aislada en el Firewall que no pueda acceder a ninguna otra red. A la cual se hará el NATEO de los puertos los cuales estará escuchando.
Es importante destacar que estos requisitos son superiores a los mínimo necesarios, pero proporciona un margen de seguridad para un funcionamiento fluido y sin interrupciones. La elección de Debian 12 como sistema operativo base asegura la compatibilidad y estabilidad de T-Pot, ya que esta optimizando para funcionar en esta distribución.

Instalación

Instalar T-Pot es la cosa más sencilla del mundo ya que solo hay que ejecutar un par de comandos y estará todo funcional. Lo que se debe hacer es tener una máquina totalmente virgen es decir S.O recién instalado para evitar problemas al momento de instalar.
Los comandos son los siguientes (La instalación se debe llevar acabo con un usuario con permisos de administración pero **JAMÁS CON ROOT**, ya que T-Pot no esta permitido para instalarse como root):

Primero antes que nada obviamente actualizar la máquina

```
sudo apt update && sudo apt upgrade -y
```

Una vez actualizado se deben instalar diferentes dependencias para ser utilizadas más adelante.

```
sudo apt install git -y && sudo apt install curl -y && sudo apt install docker-compose -y
```
Se usa && para que en cuanto acabe el comando anterior se ejecute el siguiente comando esto para hacer una cadena de comandos para poder hacer la instalación más rápida

Ahora teniendo todas las dependencias necesarias se procederá con la instalación y configuración de T-Pot. Se deberán ejecutar los siguientes comandos:
```
git clone https://github.com/telekom-security/tpotce && cd tpotce && ./install.sh
```

Esta cadena de comandos hará lo siguiente:

1. Clonará el repositorio de T-Pot (tpotce), ya que en el se encuentran todas las herramientas para su implementación.
2. Una vez se ha clonado el repositorio se moverá a la carpeta llamada tpotce
3. Por último ejecutará el script para instalar T-Pot, es posible que pida la contraseña del usuario ya que para algunas cosas necesita permiso de administrador y en caso de que el usuario no tenga permisos de admin pedirá la contraseña del usuario root y luego se ejecutaŕa como el usuario normal.

Ahora bien una vez empiece el script a funcionar irá descargando dependencias que necesita, también cambiará el puerto del SSH del 22 64295.
También llegados un punto preguntará que tipo de instalación se requiere estas son:

Hive (h)
Esta es la instalación estándar de T-Pot. Incluye todos los componentes necesarios para una configuración completa, incluyendo la interfaz web, ElasticSearch y Kibana. También proporciona lo necesario para una configuración distribuida con sensores.

Sensor (s)
Optimizada para una instalación distribuida. No incluye la interfaz web (WebUI), ElasticSearch ni Kibana. Es ideal para desplegar múltiples sensores en una red.

LLM (l)
Esta instalación utiliza HoneyPots basados en modelos de lenguaje (LLM) específicamente **Beelzebub** y **Galah**. **Requiere Ollama** (recomendado) o una **suscripción a ChatGPT.**

Mini (i)
Una instalación reducida que permite ejecutar más de 30 HoneyPots con solo un par de demonios de HoneyPot. Es útil para entornos con recursos limitados.

Mobile (m)
Incluye todo lo necesario para ejecutar T-Pot Mobile, que está disponible por separado. Esta opción está diseñada específicamente para entornos móviles.

Tarpit (t)
Esta instalación está diseñada para alimentar datos interminablemente a atacantes, bots y escáneres. También ejecuta un HoneyPot de Denegación de Servicio (ddospot). Es útil para ralentizar y frustrar a los atacantes.

Se deberá elegir la configuración preferida en este caso recomiendo usar la tipo **Hive (h),** ya que a mi parecer es la más completa para el tema de HoneyPots.
En el proceso pedirá configurar un usuario y contraseña para el control de la web donde se podrán ver los logs mediante dashboards con Kibana en el puerto 64297

Posibles problemas

En caso de que existan problemas al momento de instalar en el que el Log indica el nombre de rlimit, es porque

1. Se está intentando instalar T-Pot en un contenedor cosa que no es posible apesar de tener los recursos necesarios

2. Que la máquina desde la cuál se quiere instalar T-Pot no tiene los recursos suficientes.

Una vez se ha Terminado de instalar T-Pot se deberá reiniciar la máquina host. Al estar otra vez en la máquina se deberán ejecutar el siguiente comando para comprobar que todo funciona bien:

```
sudo docker ps
```

Esto se hace con el fin de comprobar que todos los contenedores estén UP.

En caso de que el comando anterior no muestre ningún contenedor se deberá ejecutar lo siguiente dentro de la carpeta tpotce

```
sudo docker-compose up
```

Este comando se ejecuta con el fin de que se vuelva a mandar el inicio a todos los contenedores con los HoneyPots necesarios para la prueba, ahora bien una vez se tiene todo bien configurado se va a proceder con la práctica.

Últimos pasos

Ahora lo que quedará hacer es lo siguiente

1. Entrar a la web de T-Pot: **https://IP_MÁQUINA_HONEY:6427.** Se deberá entrar en Kibana
2. Publicar al exterior los puertos por los que se quieren recibir ataques hacia la máquina con el T-Pot instalado.
3. Y por último esperar los ataques de los desgraciados **hackers.**

Para ver mejor los ataques que realizan los atacantes se pueden ver en la siguiente ruta:

```
~/tpotce/data/honeypotelegido/log/puertopublicado.log
```

Ejemplo:

```
~/tpotce/data/ddospot/log/ntpot.log
```