

Honeypots: Implementación y análisis

OBJETIVOS:

- ENTENDER QUE ES UN HONEYPOT
- APRENDER COMO CONFIGURAR T-POT
- ANALIZAR DATOS Y EXTRAER CONCLUSIONES



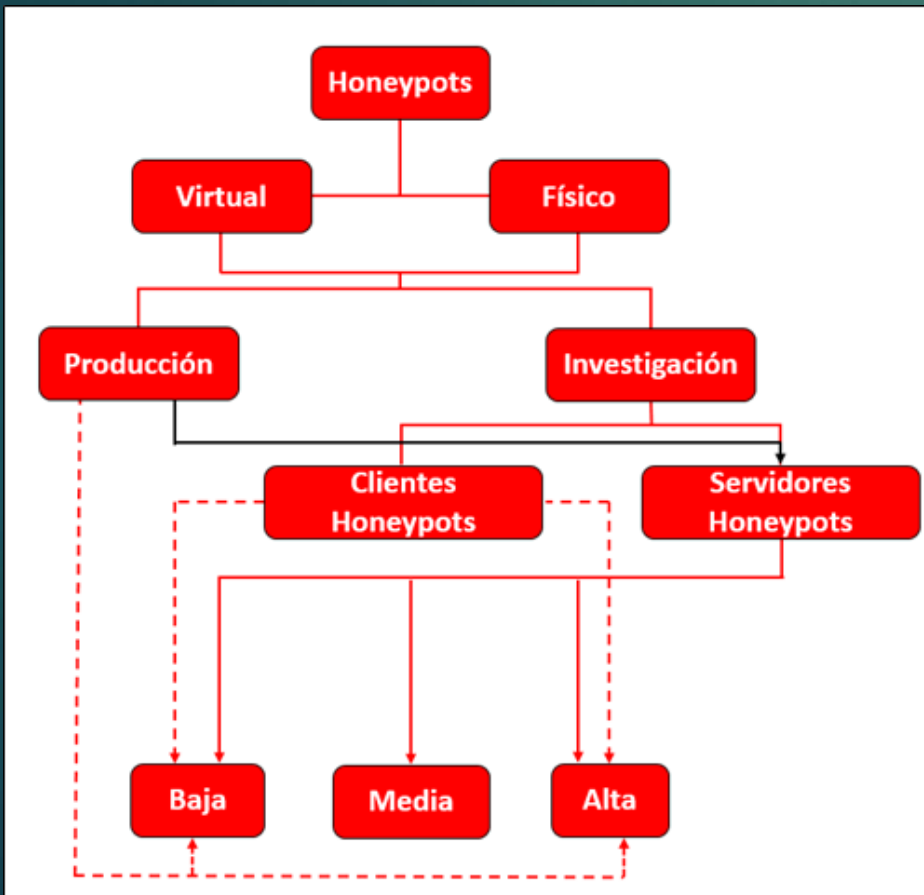
Definición y propósitos principales

- ▶ ¿Qué es un honeypot?
 - ▶ Un honeypot es un sistema o dispositivo de red diseñado para atraer y engañar a los atacantes, haciéndoles creer que es un objetivo vulnerable, con el fin de detectar, estudiar y mitigar sus actividades maliciosas sin comprometer la seguridad de la red real.
- ▶ Propósitos principales
 - ▶ **Detectar ataques:** Identificar intentos de intrusión en una red.
 - ▶ **Estudiar técnicas:** Analizar métodos y herramientas utilizadas por los atacantes.
 - ▶ **Distraer atacantes:** Desviar la atención de los atacantes de los verdaderos sistemas críticos.



Tipos de honeypots

Tradicionalmente las honeypots se clasifican en honeypots de alta y baja interacción, aunque es posible encontrar clasificaciones con más niveles según la interacción con los atacantes.



▶ Honeypots de Baja Interacción:

- ▶ Emulan algunos servicios y funcionalidades básicas del sistema
- ▶ Recopilan información básica y algo limitada del atacante con pocos recursos.
- ▶ Son fáciles de implementar y mantener.
- ▶ Útiles para detectar los primeros pasos de un ataque.

▶ Honeypots de Alta Interacción:

- ▶ Emulan un abanico muy amplio de servicios y comportamientos de un sistema real.
- ▶ Permiten realizar una investigación más profunda del ataque e identificar el nivel de riesgo de la amenaza, métodos y objetivo del atacante.
- ▶ Son más complejos y requieren más recursos y mantenimiento.

Ventajas y desventajas

▶ Ventajas

- ▶ Detección Temprana de Ataques
- ▶ Análisis Detallado
- ▶ Educación y Entrenamiento
- ▶ No requieren muchos recursos

▶ Desventajas

- ▶ Recursos Necesarios
- ▶ Falsos Positivos
- ▶ Mismas vulnerabilidades que los sistemas a los que emula
 - ▶ Mantenimiento constante
 - ▶ Posible punto de ataque



Honeypot Or Not?

Enter an IP to check whether it is a honeypot or a real control system:

Check for Honeypot

Introducción a T-POT

► ¿Qué es T-POT?

- T-Pot es una plataforma de honeypots de código abierto que integra múltiples honeypots en una única solución para detectar y analizar actividades maliciosas.



► Características clave:

- Multihoneypot
- Dashboard visual
- Automatización



Instalación y Configuración de T-POT

► Requisitos Previos:

- Hardware y software.
- Configuraciones de red y seguridad.

T-Pot Type	RAM	Storage
Hive	16GB	256GB SSD
Sensor	8GB	128GB SSD

100	POT-SSH-IN	64295	TCP	207.188.138.51,83.55.106.149	Any	✔ Allow
110	POT-WEB	64297	TCP	207.188.138.51,83.55.106.149	Any	✔ Allow
120	TPOT-ALL	0-64293,64298-...	TCP	Any	Any	✔ Allow
65000	AllowVnetInBound ⓘ	Any	Any	VirtualNetwork	VirtualNetwork	✔ Allow

- Pasos clave para la instalación.
- Configuraciones básicas y avanzadas.
 - Puertos, servicios y alertas.

Demostración en vivo (8-9min)

► **Demostración 1: Configuración Interna de T-POT (4 minutos)**

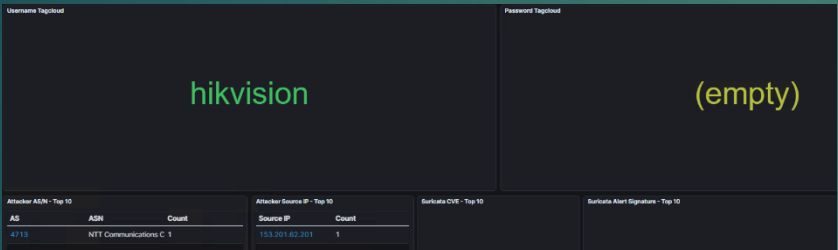
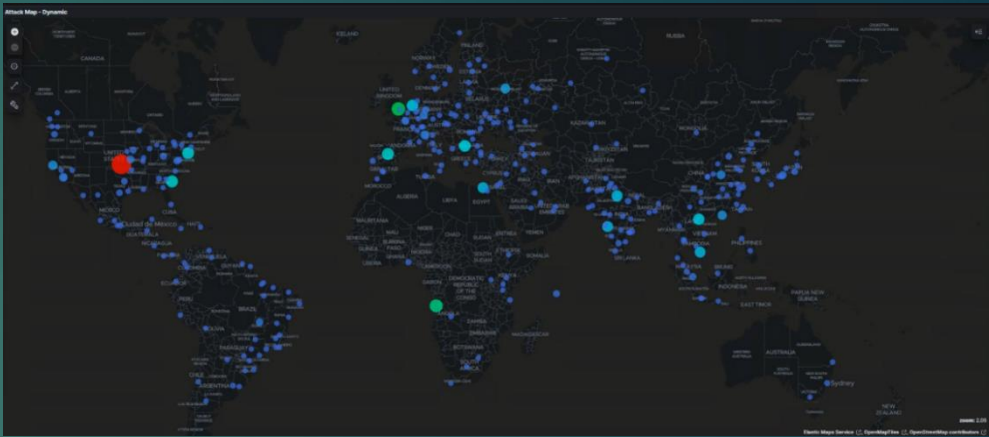
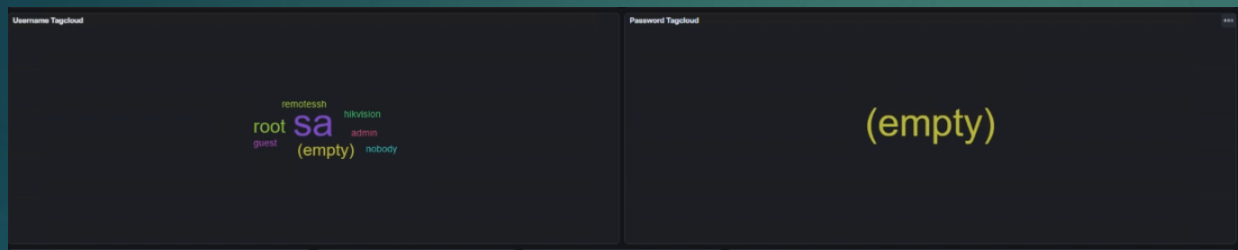
- Mostrar la interfaz de configuración.
- Explicar brevemente los componentes principales.
- Enseñar cómo se configuran los servicios y alertas.

► **Demostración 2: Resultados del Honeypot (4 minutos)**

- Mostrar datos recopilados (intentos de acceso, tipos de ataques, IPs de origen).
- Utilizar gráficos y estadísticas generados.
- Explicar la interpretación de los resultados y patrones observados.

Conclusiones y Trabajo Futuro

- ▶ Resumen de hallazgos importantes.
- ▶ Recomendaciones y posibles mejoras futuras.



root

---fuck_you---

Src IP - Top 10 - Dynamic	
Source IP	Count
113.160.130.153	488
183.81.169.238	296
121.35.9.58	292
120.236.227.194	204
122.202.213.237	138
49.213.157.179	127
202.126.212.118	117
170.64.175.175	105
103.79.27.119	65
117.219.93.172	61
Rows per page: 10 < 1 >	

Cowrie Input - Top 10	
Command Line Input	Count
shell	72
system	70
enable	36
sh	36
ping; sh	30
while read i	11
apt install sudo curl -y	10
apt update	10
/ip cloud print	6
dd bs=52 count=1 if=s cat .s while read i; do	5
Rows per page: 10 < 1 >	

Cowrie - Top Downloads		
Filename	T-Pot Path (/data/cowrie/downloads)	Count
sshd	dl/7c4d16ae0e92dfc65fde6e700929fefaaf4a42	1
sshd	dl/94f2e4d8d4436874785cd14e6e6d403507b1	1

Cowrie - Top Downloads		
Filename	T-Pot Path (/data/cowrie/downloads)	Count
sshd	dl/7c4d16ae0e92dfc65fde6e700929fefaaf4a42	1
sshd	dl/94f2e4d8d4436874785cd14e6e6d403507b1	1

Referencias

- ▶ <https://github.com/telekom-security/tpotce?tab=readme-ov-file#choose-your-distro>
- ▶ <https://www.linkedin.com/pulse/setup-t-pot-honeypot-azure-less-than-30-minutes-sigmund/>
- ▶ <https://latam.kaspersky.com/resource-center/threats/what-is-a-honeypot>
- ▶ <https://www.incibe.es/incibe-cert/blog/honeypots-industriales#:~:text=Tradicionalmente%20las%20honeypots%20se%20clasifican,la%20interacci%C3%B3n%20con%20los%20atacantes.>
- ▶ <https://www.cibernicola.es/esquemas/othp.html>
- ▶ <https://www.shodan.io/>



ChatGPT

Preguntas

