🛠️ Tutorial de Instalación y Configuración de SOTYPOT

Autor: David Hernández Jiménez
Fecha de Entrega: 04 de mayo de 2025

IES CIUDAD JARDÍN

🗒️ Índice

1. *Introducción*
2. *¿Qué es SOTYPOT?*
3. *Requisitos del sistema*
4. *Preparación del entorno*
5. *Descarga del repositorio*
6. *Instalación de T-Pot CE modificada (SOTYPOT)*
7. *Configuración de red y puertos*
8. *Acceso a la interfaz web*
9. *Implementación de la Landing Page con Docker*
10. *Pruebas y validación*
11. *Posibles errores y soluciones*
12. *Personalización y mejoras*
13. *Conclusión*
14. *Anexos y capturas*

1. Introducción

Este tutorial documenta de forma detallada el proceso de instalación, configuración y despliegue de **SOTYPOT**, una plataforma de honeypots adaptada a entornos educativos como parte de un Proyecto Final de Grado (TFG) en ASIR de David Hernández Jiménez.

---

2. ¿Qué es SOTYPOT?

SOTYPOT es una versión personalizada de T-Pot CE con una interfaz localizada al español, una landing page informativa accesible por navegador, y una mejor orientación a nivel pedagógico. Tiene como objetivo ofrecer una plataforma de ciberseguridad pasiva para detectar y registrar ataques reales en entornos simulados.

---

3. Requisitos del sistema

Componente	Requisito mínimo
CPU	4 núcleos
RAM	8 GB
Almacenamiento	128 GB SSD
SO	Ubuntu 24.04.1 Live Server o superior (64-bit)
Red	Conexión sin filtrado de puertos

---

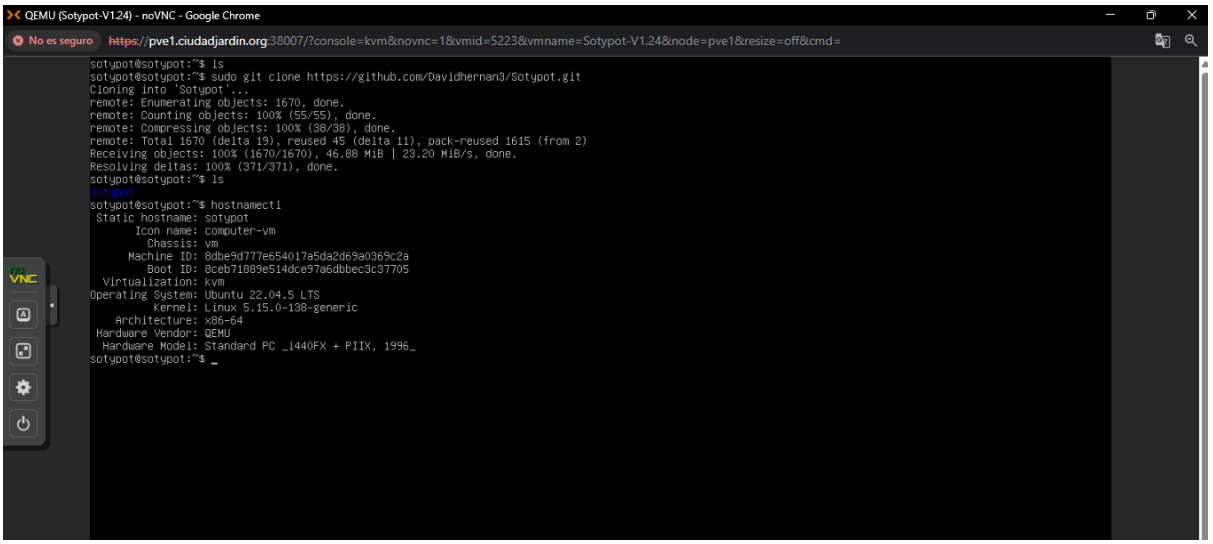
4. Preparación del entorno

```
sudo apt update && sudo apt upgrade -y
sudo apt install git curl docker.io docker-compose -y
```

---

5. Descarga del repositorio

```
git clone https://github.com/descambiado/Sotypot.git
cd SOTYPOT
```



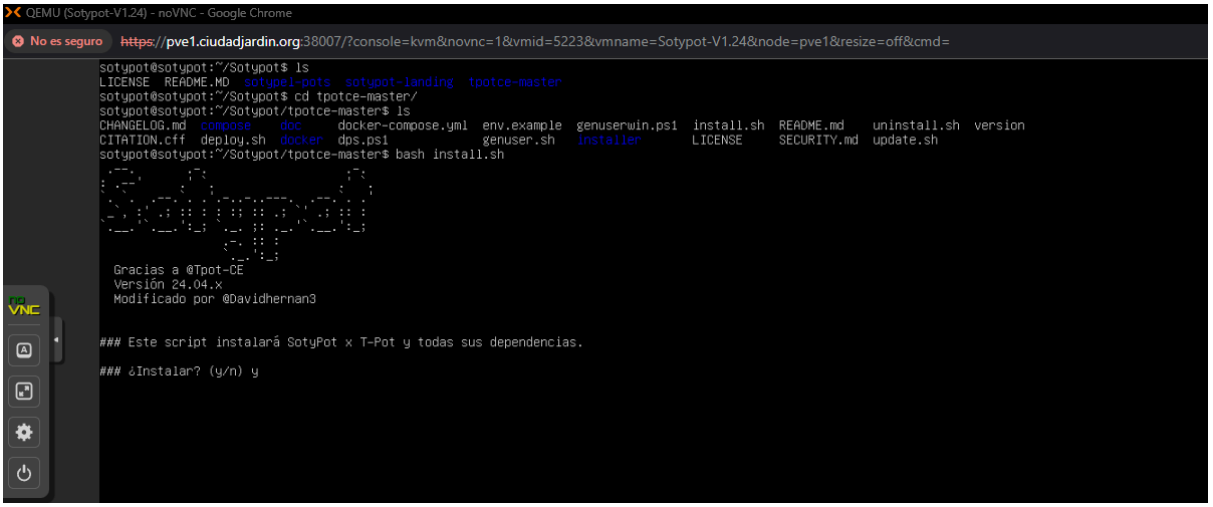
---

6. Instalación de SOTYPOT

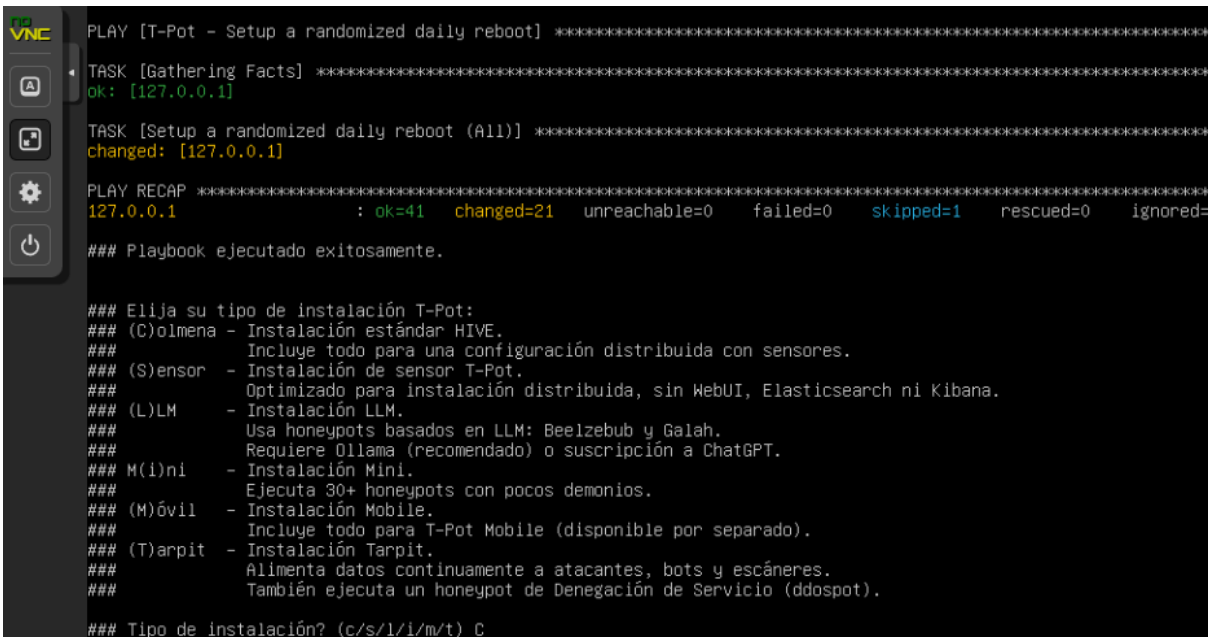
Lanzar el script automático de instalación:

Dentro de ./Sotypot/Tpotce-master$

bash install.sh



Durante el proceso se instalarán todos los contenedores y servicios requeridos.



---

7. Configuración de red y puertos

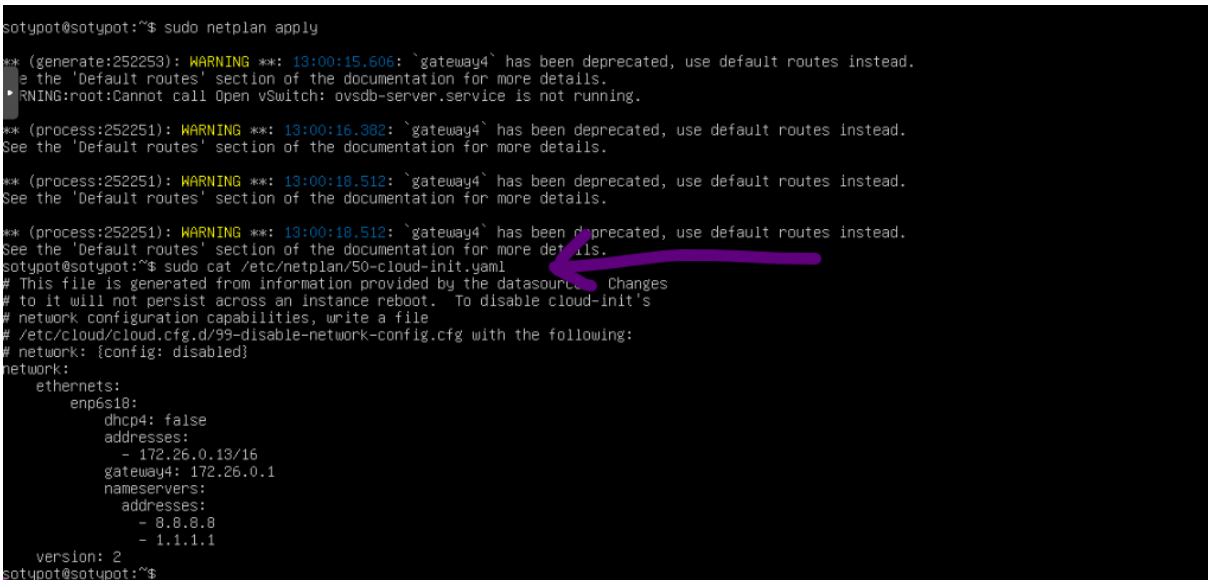
- Interfaz web de T-Pot:
    - `https://<IP_LOCAL>:64297`

- Dashboard (Kibana): mismo puerto
- Landing personalizada (Insa:

```
ports:
      - "8888:80"    # HTTP (redirige a HTTPS)
      - "8887:443"   # HTTPS seguro con auth básica
```

⚠️ Si algún puerto ya está en uso, edita el `docker-compose.yml` y cambia `8887:443` a otro puerto.

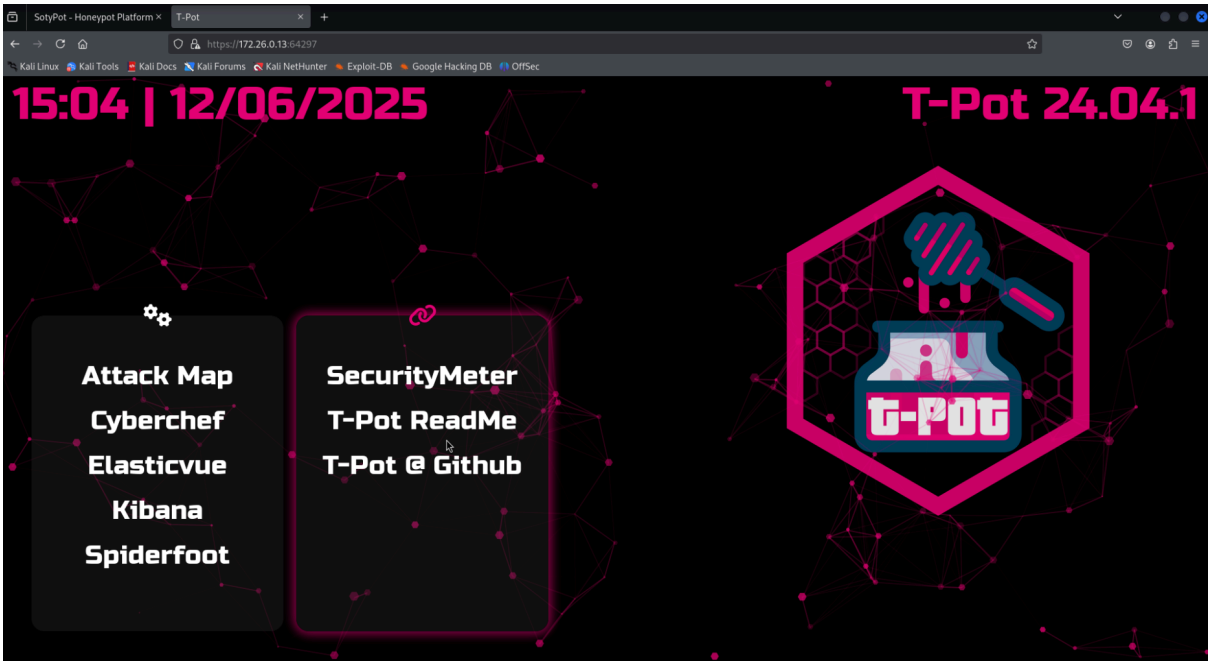
(Intentar configurar la ip fija a 172.26.0.13, despues de la instalación)



8. Acceso a la interfaz web

Una vez finalizada la instalación de TPOT, pasaremos a el punto 9 para el landing personalizado de sotypot, hacemos una prueba de que tpot funciona correctamente:

- Abrir navegador TPOT: `https://<tu-ip>:64297`
- Usuario: la definida durante instalación
- Contraseña: la definida durante instalación



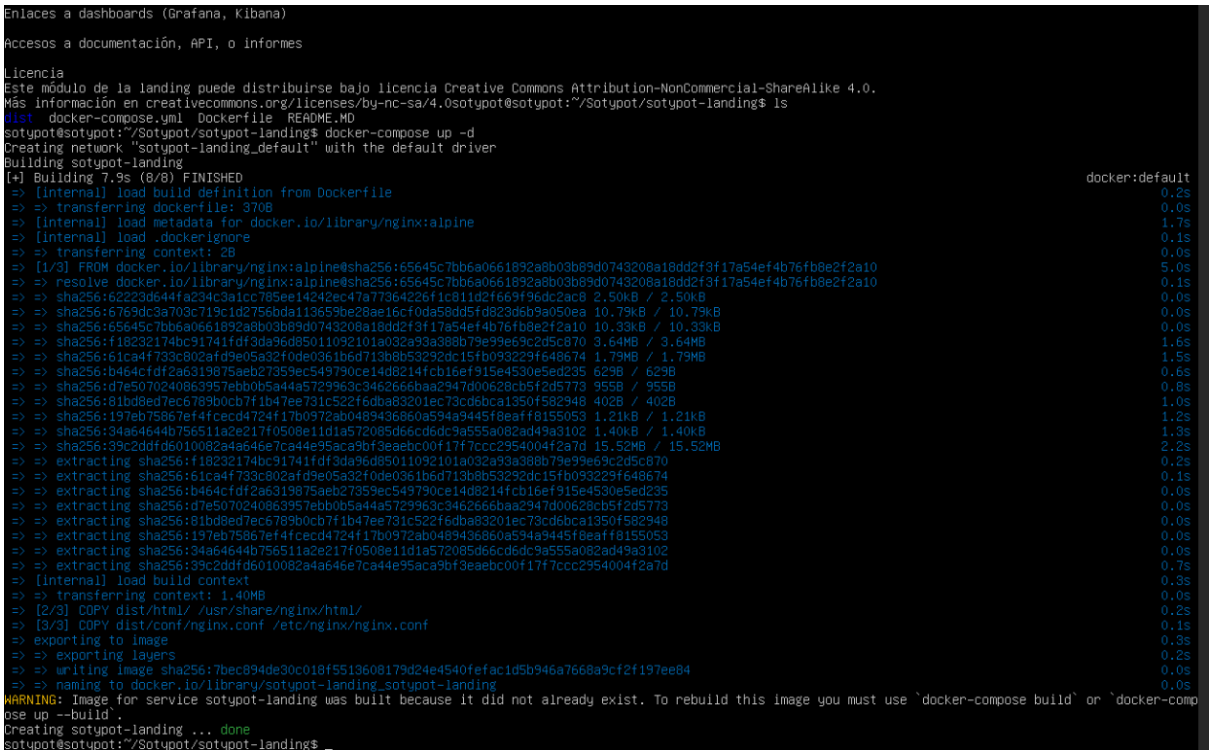
9. Implementación de la Landing Page con Docker

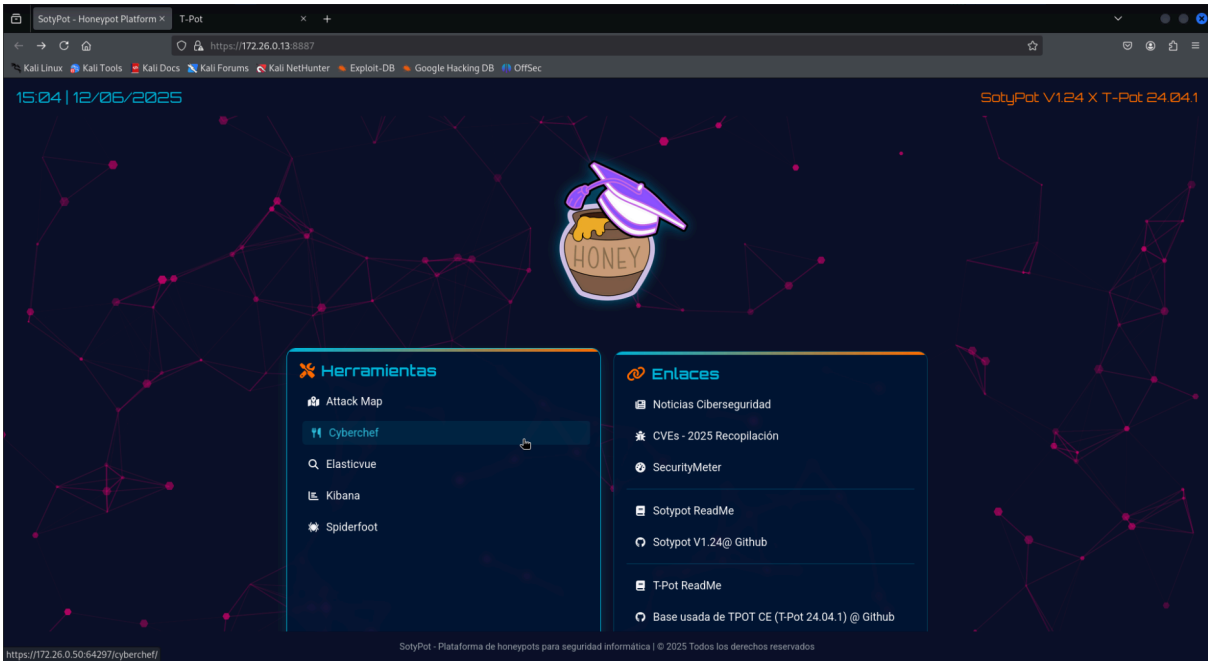
1.`cd sotypot-landing`

2. `Ejecuta sotypot-landing/create-setup.sh`
   `(Puedes editarlo, son archivos de configuración SSL Y Password)`

3.`docker-compose up -d`

Asegúrate de que `index.html` esté en `dist/html/`. Si lo modificas, reinicia el contenedor para aplicar los cambios.





https://172.26.0.13:8887

---

11. Posibles errores y soluciones

Problema	Solución
404 en la landing	Verifica que `index.html` esté en el directorio correcto (`dist/html/`)
Puerto en uso	Cambia el puerto en `docker-compose.yml`
Kibana no carga	Verifica servicio Elasticsearch y reinicia

---

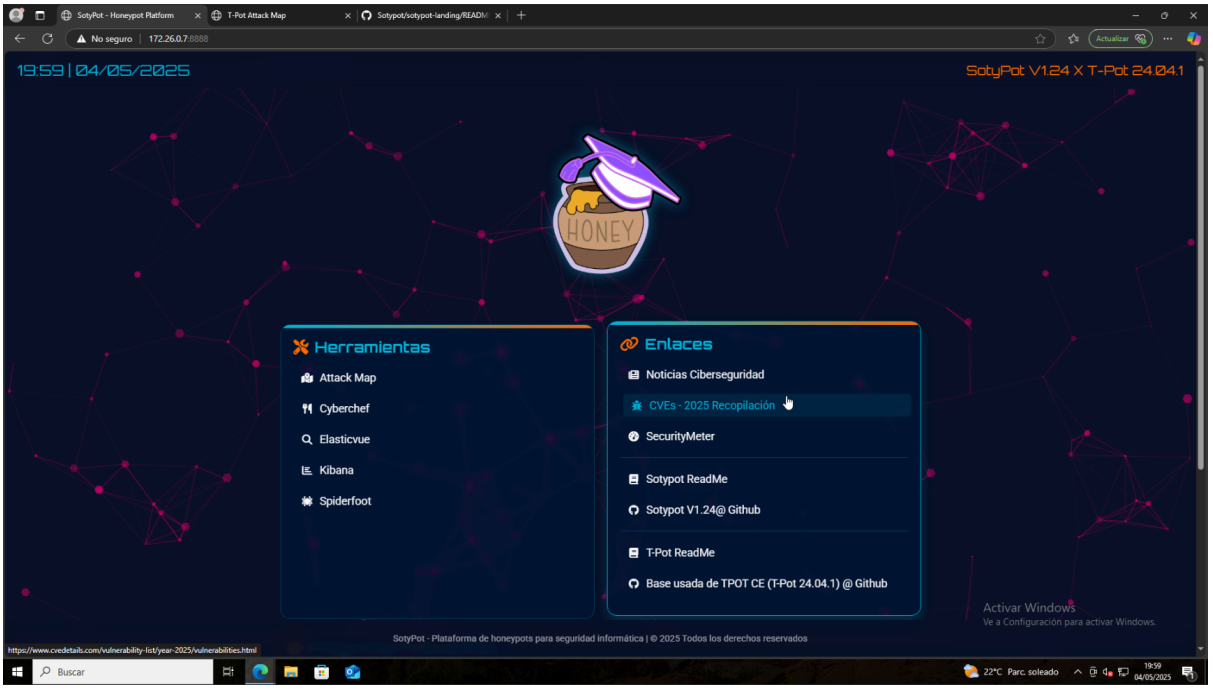
12. Personalización y mejoras

- Puedes modificar los honeypots editando sus archivos YAML.
- Personaliza dashboards de Kibana exportando/creando nuevos.
- Cambia el aspecto de la landing con HTML/CSS en `dist/html/index.html`.

---

13. Conclusión

SOTYPOT permite visualizar y analizar amenazas reales en redes corporativas simuladas. Su despliegue es automático y su uso está pensado para formaciones prácticas en ciberseguridad. La personalización y modularidad del sistema lo convierten en una herramienta escalable y educativa.



Este trabajo se distribuye bajo la licencia Creative Commons