

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

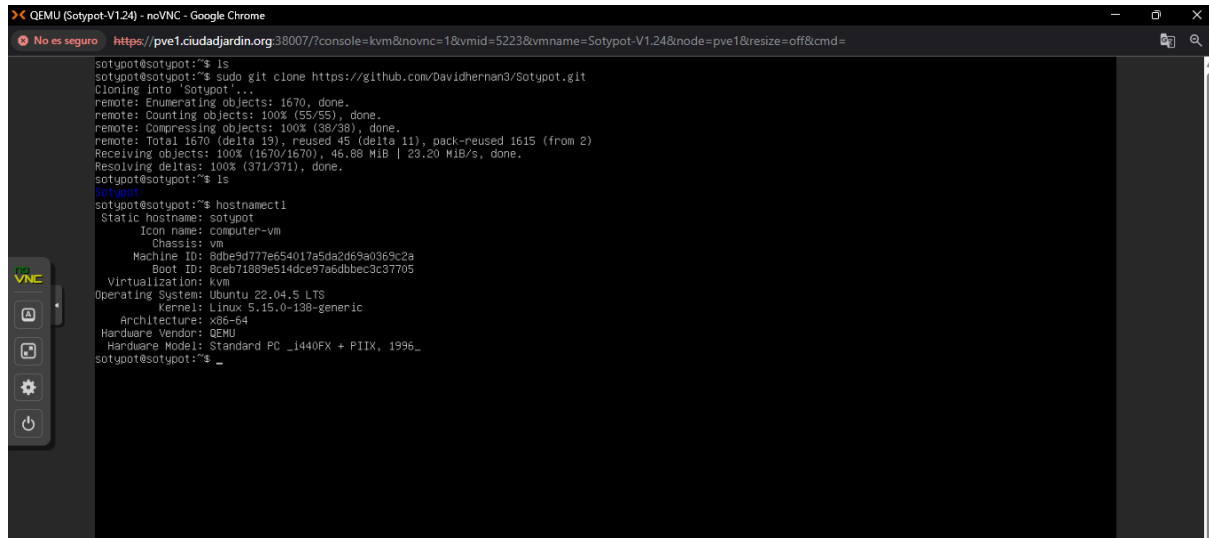
Componente	Requisito mínimo
CPU	4 núcleos
RAM	8 GB
Almacenamiento	128 GB SSD
SO	Ubuntu 24.04.1 Live Server o superior (64-bit)
Red	Conexión sin filtrado de puertos

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 S0TYP0T
```

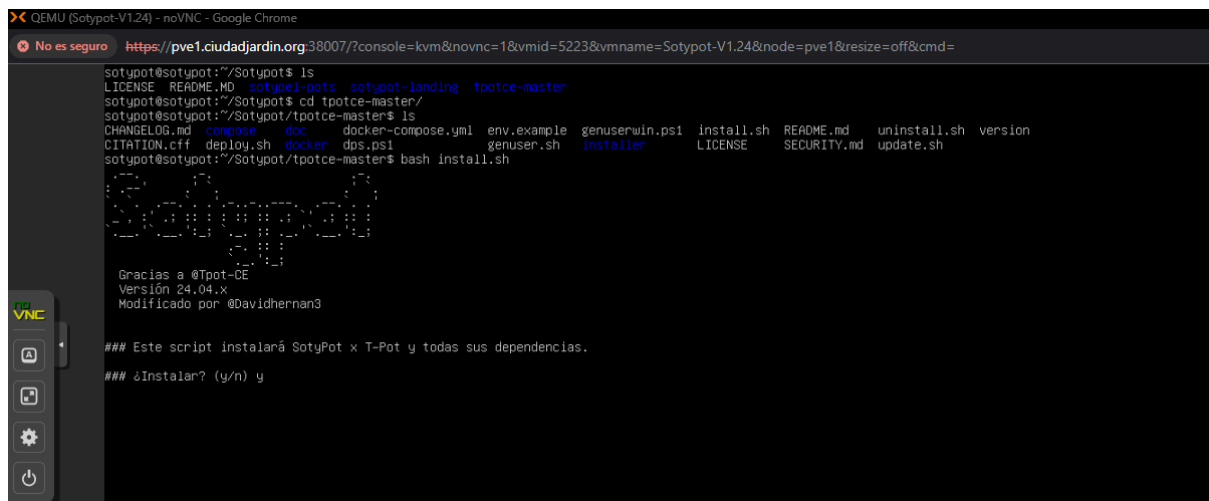


6. Instalación de SOTYPOT

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.

```

PLAY [T-Pot - Setup a randomized daily reboot] *****
TASK [Gathering Facts] *****
ok: [127.0.0.1]

TASK [Setup a randomized daily reboot (All)] *****
changed: [127.0.0.1]

PLAY RECAP *****
127.0.0.1 : ok=41 changed=21 unreachable=0 failed=0 skipped=1 rescued=0 ignored=

### Playbook ejecutado exitosamente.

### Elija su tipo de instalación T-Pot:
### (C)olmena - Instalación estándar HIVE.
###           Incluye todo para una configuración distribuida con sensores.
### (S)ensor - Instalación de sensor T-Pot.
###           Optimizado para instalación distribuida, sin WebUI, Elasticsearch ni Kibana.
### (L)LM - Instalación LLM.
###           Usa honeypots basados en LLM: Beelzebub y Galah.
###           Requiere Ollama (recomendado) o suscripción a ChatGPT.
### M(i)ni - Instalación Mini.
###           Ejecuta 30+ honeypots con pocos demonios.
### (M)óvil - Instalación Mobile.
###           Incluye todo para T-Pot Mobile (disponible por separado).
### (T)arpit - Instalación Tarpit.
###           Alimenta datos continuamente a atacantes, bots y escáneres.
###           También ejecuta un honeypot de Denegación de Servicio (ddospot).

### Tipo de instalación? (c/s/l/i/m/t) C

```

7. Configuración de red y puertos

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

```

### Verifique posibles conflictos de puertos con honeypots.
### Aunque SSH está configurado, otros servicios como
### SMTP, HTTP, etc. podrían impedir el inicio de Sotpot y T-Pot.

Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address   Foreign Address  State       User        Inode         PID/Program name
tcp        0      0 0.0.0.0:64295    0.0.0.0:*        LISTEN      0           49760         5308/sshd: /usr/sbi
tcp6       0      0 :::64295        :::*              LISTEN      0           49762         5308/sshd: /usr/sbi
udp        0      0 172.26.0.7:68   0.0.0.0:*        101         59509         680/systemd-network

### Instalación completada. Reinicie el sistema y reconéctese via SSH al puerto tcp/64295.

sotypot@sotypot:~/Sotypot/tpotce-master$

```

- 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)

```
sotypot@sotypot:~$ sudo netplan apply

** (generate:252253): WARNING **: 13:00:15.606: `gateway4` has been deprecated, use default routes instead.
See the 'Default routes' section of the documentation for more details.
* RNING:root:Cannot call Open vSwitch: ovsdb-server.service is not running.

** (process:252251): WARNING **: 13:00:16.382: `gateway4` has been deprecated, use default routes instead.
See the 'Default routes' section of the documentation for more details.

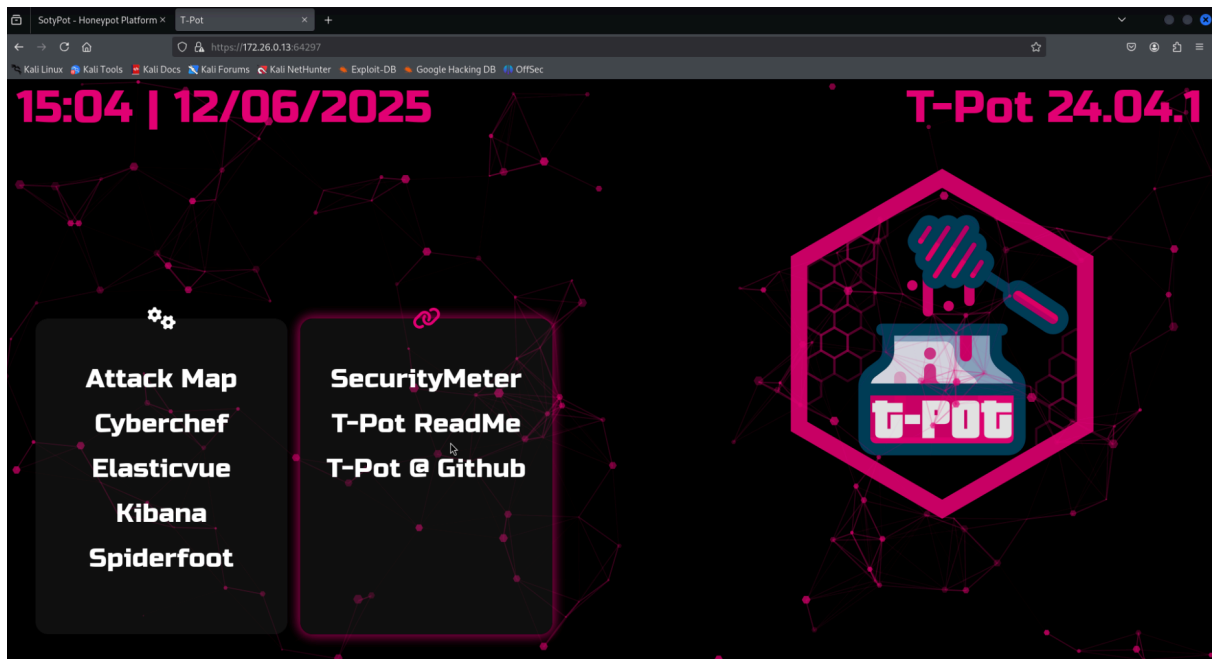
** (process:252251): WARNING **: 13:00:18.512: `gateway4` has been deprecated, use default routes instead.
See the 'Default routes' section of the documentation for more details.

** (process:252251): WARNING **: 13:00:18.512: `gateway4` has been deprecated, use default routes instead.
See the 'Default routes' section of the documentation for more details.
sotypot@sotypot:~$ sudo cat /etc/netplan/50-cloud-init.yaml
# This file is generated from information provided by the datasource.  Changes
# to it will not persist across an instance reboot.  To disable cloud-init's
# network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
  ethernets:
    enp6s18:
      dhcp4: false
      addresses:
        - 172.26.0.13/16
      gateway4: 172.26.0.1
      nameservers:
        addresses:
          - 8.8.8.8
          - 1.1.1.1
  version: 2
sotypot@sotypot:~$
```

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

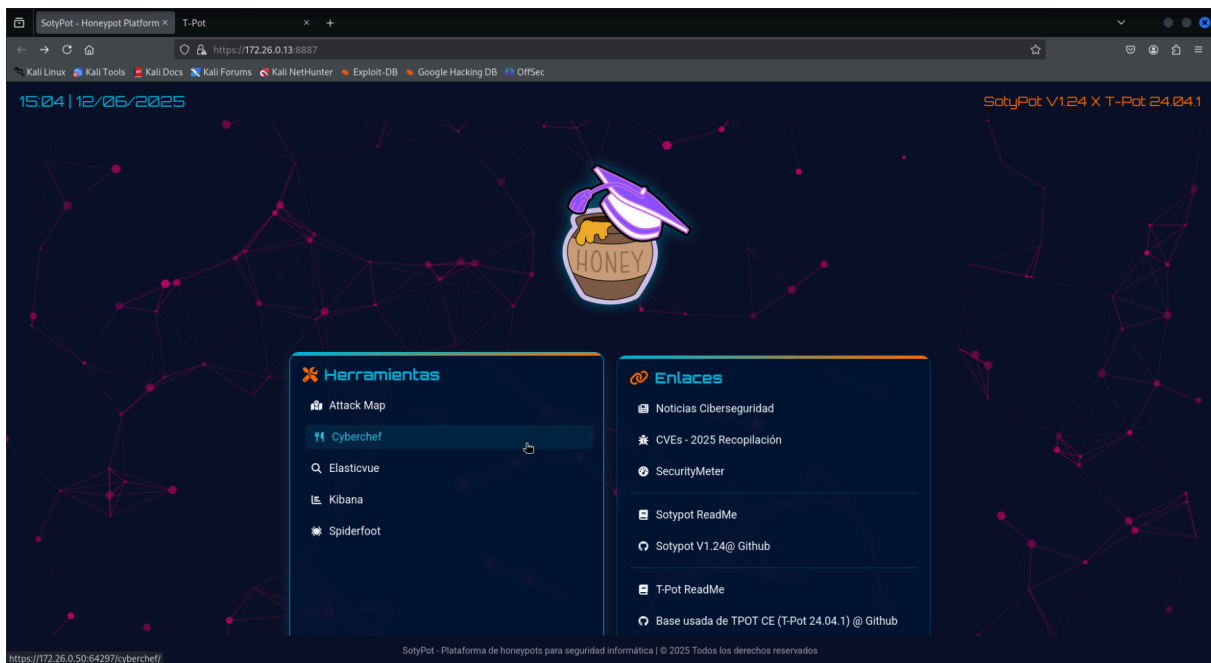
2. Ejecuta sotypot-landing/create-setup.sh

(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.

```
Enlaces a dashboards (Grafana, Kibana)
Accesos a documentación, API, o informes
Licencia
Este módulo de la landing puede distribuirse bajo licencia Creative Commons Attribution-NonCommercial-ShareAlike 4.0.
Más información en creativecommons.org/licenses/by-nc-sa/4.0sotypot@sotypot:~/Sotypot/sotypot-landing$ ls
dist  docker-compose.yml  Dockerfile  README.md
sotypot@sotypot:~/Sotypot/sotypot-landing$ docker-compose up -d
Creating network "sotypot-landing_default" with the default driver
Building sotypot-landing
[+] Building 7.9s (8/8) FINISHED
=> [internal] load build definition from Dockerfile
=> => transferring dockerfile: 370B
=> [internal] load metadata for docker.io/library/nginx:alpine
=> [internal] load .dockerignore
=> => transferring context: 2B
=> [1/3] FROM docker.io/library/nginx:alpine@sha256:65645c7bb6a0661892a8b03b89d0743208a18dd2f3f17a54ef4b76fb8e2f2a10
=> => resolve docker.io/library/nginx:alpine@sha256:65645c7bb6a0661892a8b03b89d0743208a18dd2f3f17a54ef4b76fb8e2f2a10
=> => sha256:62223d644fa234c3a1cc785ee14242ec47a77364226f1c811d2f669f96dc2ac8 2.50kB / 2.50kB
=> => sha256:6769d39103c719c1d275bda113559b28eef1c40a68bd5fd822d6b9a050ea 10.79kB / 10.79kB
=> => sha256:65645c7bb6a0661892a8b03b89d0743208a18dd2f3f17a54ef4b76fb8e2f2a10 10.33kB / 10.33kB
=> => sha256:f18232174bc91741fd1f3da96d85011092101a032a93a388b79e99e69c2d5c870 3.64MB / 3.64MB
=> => sha256:61cadf733c802afd9e05a32f0de0361b6d713b8b53292dc15fb093229f648674 1.79MB / 1.79MB
=> => sha256:b464cfd12a6319875aeb27359ec549790ce14d8214fcb16ef915e4530e5ed235 629B / 629B
=> => sha256:d7e5070240863957eb0b05a44a5729963c3462666baa2947d00628cb5f2d5773 955B / 955B
=> => sha256:81bd8ed7ec6789b0cb7f1b47ee731c522f6dba83201ec73cd6bca1350f582948 402B / 402B
=> => sha256:197eb75867ef4fcedd4724f17b0972ab0489436860a594a9445f8eaff8155053 1.21kB / 1.21kB
=> => sha256:34a64644b756511a2e217f0508e11d1a572085d66cd6dc9a555a082ad49a3102 1.40kB / 1.40kB
=> => sha256:39c2ddfd6010082a4a646e7ca44e95aca9bf3eae00f17f7ccc2954004f2a7d 15.52MB / 15.52MB
=> => extracting sha256:f18232174bc91741fd1f3da96d85011092101a032a93a388b79e99e69c2d5c870 0.2s
=> => extracting sha256:61cadf733c802afd9e05a32f0de0361b6d713b8b53292dc15fb093229f648674 0.1s
=> => extracting sha256:b464cfd12a6319875aeb27359ec549790ce14d8214fcb16ef915e4530e5ed235 0.0s
=> => extracting sha256:d7e5070240863957eb0b05a44a5729963c3462666baa2947d00628cb5f2d5773 0.0s
=> => extracting sha256:81bd8ed7ec6789b0cb7f1b47ee731c522f6dba83201ec73cd6bca1350f582948 0.0s
=> => extracting sha256:197eb75867ef4fcedd4724f17b0972ab0489436860a594a9445f8eaff8155053 0.0s
=> => extracting sha256:34a64644b756511a2e217f0508e11d1a572085d66cd6dc9a555a082ad49a3102 0.0s
=> => extracting sha256:39c2ddfd6010082a4a646e7ca44e95aca9bf3eae00f17f7ccc2954004f2a7d 0.7s
=> [internal] load build context
=> => transferring context: 1.40MB
=> [2/3] COPY dist/html/ /usr/share/nginx/html/
=> [3/3] COPY dist/conf/nginx.conf /etc/nginx/nginx.conf
=> exporting to image
=> exporting layers
=> => writing image sha256:7bec894de30c018f5513608179d24e4540fefac1d5b946a7668a9cf2f197ee84
=> => naming to docker.io/library/sotypot-landing_sotypot-landing
WARNING: Image for service sotypot-landing was built because it did not already exist. To rebuild this image you must use `docker-compose build` or `docker-compose up --build`.
Creating sotypot-landing ... done
sotypot@sotypot:~/Sotypot/sotypot-landing$
```

<https://172.26.0.13:8887>

11. Posibles errores y soluciones

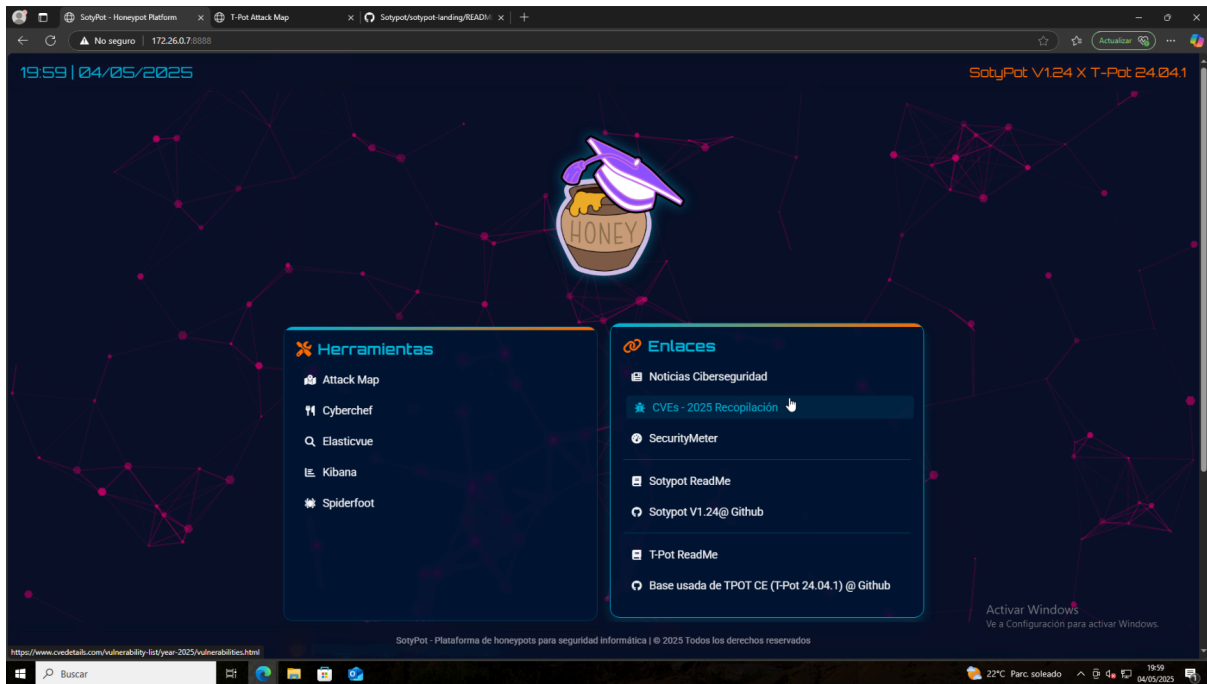
Problema	Solución
404 en la landing	Verifica que <code>index.html</code> esté en el directorio correcto (<code>dist/html/</code>)
Puerto en uso	Cambia el puerto en <code>docker-compose.yml</code>
Kibana no carga	Verifica servicio Elasticsearch y reinicia

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

Attribution-NonCommercial-ShareAlike 4.0 International.

(<http://creativecommons.org/licenses/by-nc-sa/4.0/>)