GUÍA DE INSTALACIÓN · CERT.GT

Sensor comunitario T-Pot

Versión 1.0 · Revisada el 11 oct 2026 · TLP:CLEAR · Para: quien administre un servidor Linux

Esta guía te lleva de un servidor vacío a un sensor que reporta ataques a la red de cert.gt. Tú instalas T-Pot en modo Sensor; el equipo de cert.gt lo vincula después al nodo central (Hive). El sensor es un señuelo: sólo registra a quien lo ataca, nunca tu tráfico.

Cómo funciona

- Tu sensor expone servicios falsos (SSH, web, bases de datos) que atraen ataques automatizados.
- Cada intento se registra y se envía cifrado al nodo central de cert.gt.
- Los datos se publican agregados en el mapa en vivo y las estadísticas; nunca se muestra tu IP ni tu ubicación exacta.

Antes de empezar

- Un servidor o máquina virtual dedicada: no instales T-Pot en un equipo que ya tenga otros usos.
- Recursos recomendados por T-Pot para el tipo Sensor: 8 GB de RAM y 128 GB de disco. Confirma los valores vigentes en la documentación oficial.
- Sistema operativo recién instalado y soportado por T-Pot (Debian o Ubuntu Server, entre otros).
- Una IP pública dedicada, o una DMZ aislada. Nunca lo coloques dentro de tu red interna.
- Acceso a internet de salida y un usuario con permisos de sudo.

Paso 1 · Instala T-Pot en modo Sensor

Entra a tu servidor con un usuario normal (no root) y ejecuta:

```
git clone https://github.com/telekom-security/tpotce.git
cd tpotce/
./install.sh
```

- Cuando el instalador pregunte el tipo, elige **Sensor** (opción **S**).
- Al terminar, reinicia el servidor:

```
sudo reboot
```

Importante: después del reinicio, el SSH de administración deja de estar en el puerto 22 y pasa al **64295**. El puerto 22 queda atendido por el señuelo. Para volver a entrar:

```
ssh -p 64295 tu_usuario@ip_de_tu_sensor
```

Paso 2 · Solicita la vinculación

- Llena el formulario en **cert.gt/sensor** con la IP pública del sensor, el departamento donde está y un correo de contacto.
- El equipo de cert.gt te responde con la llave pública SSH del nodo central y el destino al que tu sensor enviará sus eventos.
- No envíes contraseñas por el formulario ni por correo.

Paso 3 · Autoriza al nodo central

El nodo central configura tu sensor de forma automatizada (Ansible) por SSH. Para permitirlo, agrega la llave pública que te enviamos al usuario de administración del sensor:

```
mkdir -p ~/.ssh && chmod 700 ~/.ssh
echo "LLAVE_PUBLICA_QUE_TE_ENVIAMOS" >> ~/.ssh/authorized_keys
chmod 600 ~/.ssh/authorized_keys
```

- Si tienes firewall, permite el puerto 64295 sólo desde la IP del nodo central que te indiquemos.
- Durante el despliegue te pediremos, por un canal acordado, que escribas tú mismo la contraseña de sudo, o que habilites sudo temporal para ese usuario.

Paso 4 · Verifica

- El equipo de cert.gt ejecuta el despliegue desde el nodo central y te confirma cuando el sensor queda registrado.
- Reinicia el sensor una vez más cuando te lo indiquemos.
- En unos minutos tus eventos empiezan a aparecer en el mapa en vivo, agregados por departamento.

Para revisar el estado de los servicios en tu sensor:

```
sudo systemctl status tpot
sudo docker ps
```

Mantenlo seguro

- No guardes información propia en el sensor ni reutilices en él contraseñas de otros sistemas.
- Bloquea la salida del sensor hacia tu red interna; sólo necesita llegar a internet y al nodo central.
- Aplica las actualizaciones de T-Pot cuando te avisemos.
- Si vas a darlo de baja, escríbenos para retirarlo del nodo central.

Si algo falla

- No puedes entrar por SSH: recuerda usar el puerto 64295.
- El instalador se detiene: verifica que el sistema esté recién instalado y con los recursos mínimos.
- El sensor no aparece en el mapa: confirma con nosotros que la vinculación terminó y que tu firewall permite la salida.
- Cualquier duda: escribe a incidentes@cert.gt con el asunto “Sensor”.

cert.gt es una iniciativa privada y comunitaria de Devel Group.

cert.gt · devel.group · Reporta un incidente en cert.gt/reportar o a incidentes@cert.gt

T-Pot es un proyecto de código abierto de Telekom Security (github.com/telekom-security/tpotce). Al instalar el sensor aceptas que los datos del señuelo se publiquen de forma agregada. Esta guía no es un documento de una entidad gubernamental.