

285 - SEGURIDAD

Pon una trampa para intrusos en tu red

Instala un señuelo (honeypot) con OpenCanary en tu propia red para enterarte si alguien intenta curiosear donde no debe.



NIVEL
Avanzado

TIEMPO
45 min

CATEGORÍA
Seguridad

WEB
soporteinformatico360.com

Un señuelo es un equipo falso que parece un servidor interesante. Nadie de tu red debería tocarlo, así que si alguien lo intenta, recibes un aviso. Es una forma sencilla de aprender cómo se defiende una red.

■ Qué necesitas

- ✓ Un equipo o máquina virtual con Ubuntu dentro de tu red
- ✓ Python 3 y conexión a Internet
- ✓ Ser el dueño de la red o tener permiso
- ✓ Conocimientos básicos de terminal

■ Paso a paso

01

Prepara el equipo

Usa un equipo viejo, una Raspberry Pi o una máquina virtual en tu propia red. No guardes en él nada importante.



02

Instala OpenCanary

Crea un entorno de Python aparte e instala OpenCanary dentro, con sus dependencias.

```
Terminal
$ sudo apt install python3-venv python3-dev build-essential libssl-dev libffi-dev
$ python3 -m venv canary && source canary/bin/activate
$ pip install opencanary
$
```

03

Crea la configuración

Este comando genera el archivo de configuración. Ábrelo y activa solo un par de servicios falsos, por ejemplo ftp y http.

Terminal

```
$ sudo $(which opencanaryd) --copyconfig
$ sudo nano /etc/opencanaryd/opencanary.conf
$ █
```

04

Arranca el señuelo

Inicia OpenCanary con permisos de administrador. A partir de ahora escuchará en los puertos que hayas activado.

Terminal

```
$ sudo $(which opencanaryd) --start
$ █
```

05

Pruébalo tú mismo

Desde otro equipo de tu casa, abre en el navegador la IP del señuelo. Debe aparecer un registro de esa visita.

Terminal

```
$ tail -f /var/tmp/opencanary.log
$ █
```

06

Recibe los avisos

En la configuración puedes añadir avisos por correo. Revisa cada alerta: si no fuiste tú, investiga qué equipo era.



■ Consejos

CONSEJO 1

Pon un nombre de equipo atractivo, como servidor-copias, para que parezca real.

CONSEJO 2

No abras el señuelo a Internet: déjalo solo dentro de tu red.

CONSEJO 3

Si salta una alerta y no sabes qué hacer, un técnico puede revisar tu red.



Importante: Haz esto solo en tu propia red o con permiso por escrito del dueño. Acceder o atacar sistemas ajenos sin permiso es delito. El señuelo sirve para detectar, nunca para atacar a nadie.

¿Prefieres que lo hagamos por ti?

Diagnóstico sin compromiso y presupuesto cerrado antes de empezar. En taller, a domicilio en Madrid o por asistencia remota.

910 117 112

soporte@soporteinformatico360.com
soporteinformatico360.com