

435 - SEGURIDAD

Detecta tráfico raro con Suricata en tu lab

Monta un detector de intrusiones en tu laboratorio y aprende a leer las alertas como un analista.



NIVEL
Avanzado

TIEMPO
60 min

CATEGORÍA
Seguridad

WEB
soporteinformatico360.com

Suricata es un sistema de detección de intrusiones gratuito y de código abierto. Vigila el tráfico de red y avisa cuando ve algo sospechoso. Practicar con él en tu laboratorio te enseña a defender una red de verdad.

■ Qué necesitas

- ✓ Una máquina virtual con Ubuntu en la última versión LTS
- ✓ Un laboratorio aislado o tu propia red
- ✓ Permisos de sudo
- ✓ Ganas de leer registros

■ Paso a paso

01

Instala Suricata

En tu máquina virtual de laboratorio, instala Suricata desde los repositorios de Ubuntu.

```
Terminal
$ sudo apt update
$ sudo apt install suricata
$
```

02

Indica tu red e interfaz

Edita /etc/suricata/suricata.yaml. En HOME_NET pon el rango de tu laboratorio y en af-packet el nombre de tu interfaz (míralo con ip a).

```
Terminal
$ ip a
$ sudo nano /etc/suricata/suricata.yaml
$
```

03

Descarga las reglas

Las reglas son los patrones que Suricata reconoce. Actualízalas y reinicia el servicio.

Terminal

```
$ sudo suricata-update
$ sudo systemctl restart suricata
$ █
```

04

Genera una alerta de prueba

Usa la página de prueba pensada para esto. Responde con un texto inofensivo que las reglas reconocen como sospechoso.

Terminal

```
$ curl http://testmynids.org/uid/index.html
$ █
```

05

Lee las alertas

Mira el registro de alertas. Verás la hora, la regla que saltó y las direcciones implicadas.

Terminal

```
$ sudo tail -f /var/log/suricata/fast.log
$ █
```

06

Aprende a investigar

Para cada alerta, pregúntate qué equipo la originó, si era esperable y qué harías en una red real. Anota tus conclusiones.



■ Consejos

CONSEJO 1

Combínalo con Wireshark para ver el detalle de cada conexión que genera una alerta.

CONSEJO 2

Actualiza las reglas con frecuencia: las amenazas cambian cada semana.

CONSEJO 3

Empieza en modo detección; bloquear tráfico requiere más experiencia.



Importante: Usa Suricata solo en tu laboratorio o en redes propias con permiso. Vigilar o atacar sistemas ajenos sin autorización es delito. Si quieres llevarlo a la red de tu empresa, hazlo con un técnico.

¿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