

424 - SEGURIDAD

Detecta ataques en tu laboratorio con Wazuh

Aprende la parte defensiva del hacking ético: monta un vigilante de seguridad que avisa de accesos raros en tus máquinas de prácticas.



NIVEL
Avanzado

TIEMPO
90 min

CATEGORÍA
Seguridad

WEB
soporteinformatico360.com

Un buen hacker ético también sabe detectar ataques. Wazuh es una plataforma libre que recoge los registros de tus equipos y te avisa cuando algo parece sospechoso. La instalarás en tu laboratorio virtual.

■ Qué necesitas

- ✓ Un laboratorio con máquinas virtuales aislado
- ✓ Una máquina virtual con Ubuntu Server y 8 GB de RAM
- ✓ Otra máquina virtual con Linux para vigilar
- ✓ Conocimientos básicos de terminal

■ Paso a paso

01

Prepara el servidor

Crea una máquina virtual con Ubuntu Server en la red aislada de tu laboratorio y actualízala.

Terminal

```
$ sudo apt update && sudo apt upgrade -y
$
```

02

Instala Wazuh

Descarga el instalador oficial y usa la opción todo en uno. Al terminar te mostrará el usuario y la contraseña del panel.

Terminal

```
$ curl -sO https://packages.wazuh.com/4.x/wazuh-install.sh
$ sudo bash ./wazuh-install.sh -a
$
```

03

Entra en el panel

Desde el navegador del laboratorio abre <https://IP-del-servidor> y entra con los datos que guardaste.



04

Instala el agente

En el panel, Deploy new agent te da los comandos para la otra máquina virtual. Cópialos allí y arranca el agente.



05

Simula un acceso fallido

Desde tu laboratorio intenta entrar por SSH en la máquina vigilada con una contraseña errónea varias veces.

06

Lee las alertas

En Threat Hunting verás las alertas de autenticación fallida. Aprende a leer qué pasó, desde dónde y cuándo.

■ Consejos

CONSEJO 1

Mantén el laboratorio en una red aislada, sin acceso a tus equipos reales.

CONSEJO 2

Haz instantáneas de las máquinas virtuales antes de cada práctica.

CONSEJO 3

Practica también con retos CTF defensivos.



Importante: Practica solo en tus equipos o en tu laboratorio. Atacar o vigilar sistemas ajenos sin permiso es delito.

¿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