

268 - LINUX Y UBUNTU

Blinda el SSH de Ubuntu con fail2ban

Bloquea de forma automática a quien prueba contraseñas una y otra vez contra el acceso remoto de tu equipo.



NIVEL
Avanzado

TIEMPO
30 min

CATEGORÍA
Linux y Ubuntu

WEB
soporteinformatico360.com

Si tienes SSH activado en un Ubuntu, habrá programas que prueben contraseñas sin parar. fail2ban vigila los intentos fallidos y bloquea durante un tiempo la IP que insiste.

■ Qué necesitas

- ✓ Ubuntu con SSH ya instalado
- ✓ Acceso físico o una consola de respaldo
- ✓ Un usuario con permisos sudo
- ✓ La IP de tu red local (por ejemplo 192.168.1.0/24)

■ Paso a paso

01

Instala fail2ban

Actualiza la lista de programas e instala fail2ban. Después actívalo para que arranque siempre.

Terminal

```
$ sudo apt update
$ sudo apt install fail2ban
$ sudo systemctl enable --now fail2ban
$
```

02

Crea tu configuración

No edites jail.conf. Crea el archivo jail.local, que se respeta en las actualizaciones.

Terminal

```
$ sudo nano /etc/fail2ban/jail.local
$
```

03

Escribe las reglas

Activa la protección de sshd, deja 5 intentos, bloquea 1 hora y añade tu red en ignoreip para no bloquearte a ti.

jail.local

```
[sshd]
-----
enabled = true
-----
maxretry = 5 bantime = 1h
-----
ignoreip = 127.0.0.1/8 192.168.1.0/24
-----
```

04

Reinicia y comprueba

Reinicia el servicio y mira el estado de la jaula sshd: verás los fallos y las IP bloqueadas.

Terminal

```
$ sudo systemctl restart fail2ban
$ sudo fail2ban-client status sshd
$ █
```

05

Endurece también SSH

En /etc/ssh/sshd_config pon PermitRootLogin no. Si ya usas claves SSH, desactiva las contraseñas y reinicia con sudo systemctl restart ssh.

06

Desbloquea si te equivocas

Si bloqueas una IP tuya por error, quítala con el comando unbanip de fail2ban-client.

Terminal

```
$ sudo fail2ban-client set sshd unb
anip 192.168.1.50
$ █
```

■ Consejos

CONSEJO 1

Si no necesitas SSH desde fuera de casa, no abras el puerto en el router.

CONSEJO 2

Combínalo con el cortafuegos ufw para dejar pasar solo lo justo.

CONSEJO 3

Si es un servidor de empresa, deja que un técnico revise la configuración.



Importante: Haz estos cambios con acceso físico al equipo o una consola de respaldo. Un error en sshd_config o en ignoreip puede dejarte fuera. Antes de desactivar contraseñas, comprueba que entras con tu clave SSH.

¿Prefieres que lo hagamos por ti?

Diagnóstico sin compromiso y presupuesto cerrado antes de empezar. soporte@soporteinformatico360.com
En taller, a domicilio en Madrid o por asistencia remota. soporteinformatico360.com

910 117 112