Fail2Ban para bloquear intentos de fuerza bruta

Objetivo

- Instalar y configurar **Fail2Ban**.
- Detectar intentos de fuerza bruta en servicios como **SSH**.
- Bloquear automáticamente direcciones IP maliciosas mediante firewall.

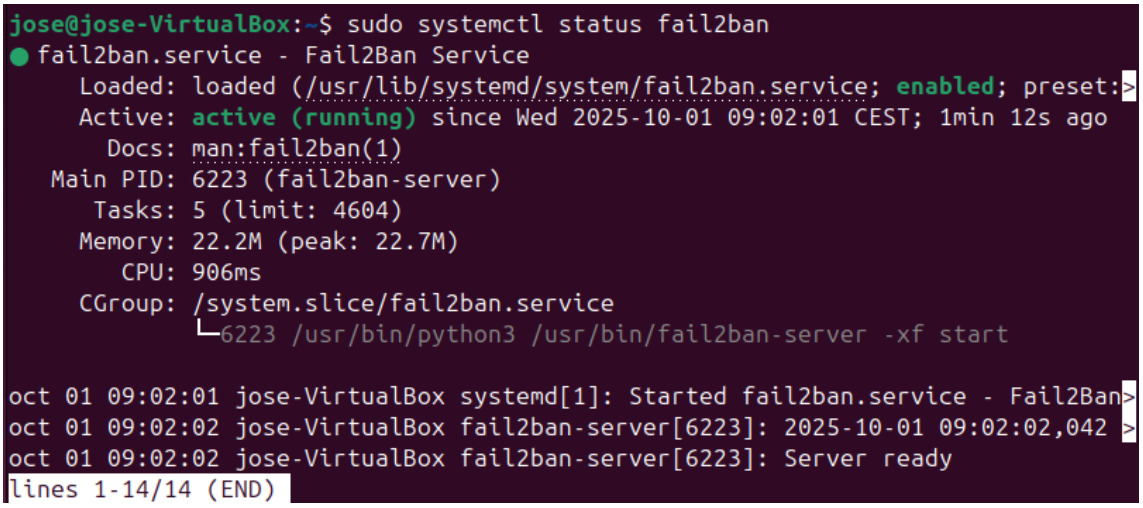
1. Preparación

- Sistema: Ubuntu/Debian (aunque también vale CentOS/RHEL con pequeñas diferencias).
- Instalar Fail2Ban:

```
sudo apt update
sudo apt install fail2ban -y
```

Comprobar estado:

```
sudo systemctl status fail2ban
```



2. Archivos de configuración

Fail2Ban no se edita directamente en /etc/fail2ban/jail.conf (ese es el *template*).
Se usa /etc/fail2ban/jail.local para configuraciones personalizadas.

Crea el archivo:

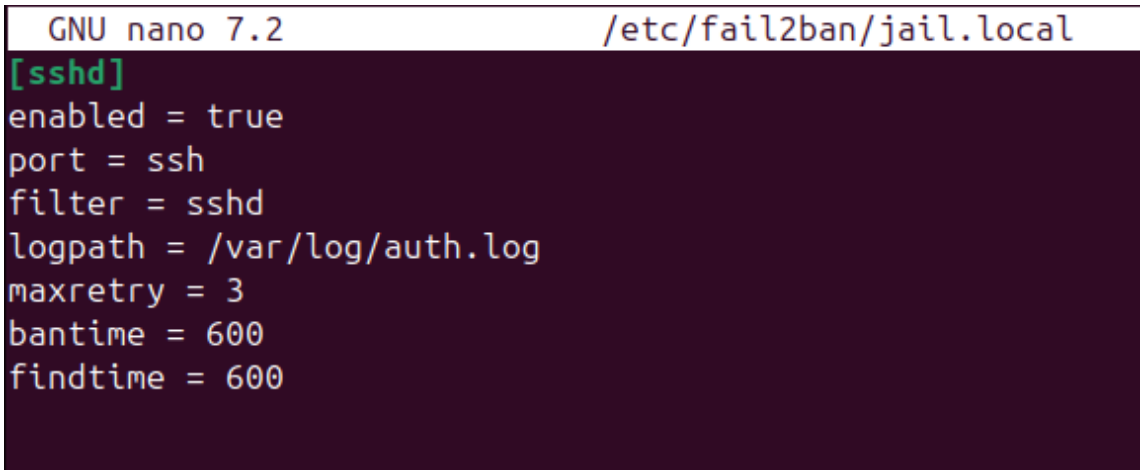
sudo nano /etc/fail2ban/jail.local

Ejemplo de configuración para **SSH**:

```
[sshd]
enabled = true
port = ssh
filter = sshd
logpath = /var/log/auth.log
maxretry = 3
bantime = 600
findtime = 600
```

Explicación:

- **enabled**: activa la protección.
- **maxretry**: nº de intentos fallidos antes de bloquear.
- **findtime**: ventana de tiempo (segundos) en la que cuentan los intentos.
- **bantime**: tiempo de bloqueo en segundos (ej. 600 = 10 minutos).



3. Reiniciar Fail2Ban

```
sudo systemctl restart fail2ban
sudo systemctl enable fail2ban
```

```
jose@jose-VirtualBox:~$ sudo systemctl enable fail2ban
Synchronizing state of fail2ban.service with SysV service script with /usr/lib/s
ystemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable fail2ban
jose@jose-VirtualBox:~$
```

Comprobar estado de las “celdas” (jails):

```
sudo fail2ban-client status
```

Debe aparecer algo como:

```
Status
|- Number of jail:      1
`- Jail list:   sshd
```

```
jose@jose-VirtualBox:~$ sudo fail2ban-client status
Status
|- Number of jail:      1
`- Jail list:   sshd
jose@jose-VirtualBox:~$
```

Y para ver detalles:

```
sudo fail2ban-client status sshd
```

```
jose@jose-VirtualBox:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
jose@jose-VirtualBox:~$
```

Pasos para habilitar SSH en Ubuntu:

1. **Instalar el servidor SSH** (si no lo tienes):

   ```
   sudo apt update
   sudo apt install openssh-server -y
   ```

2. **Verificar si el servicio está activo**:

   ```
   systemctl status ssh
   ```

   - Si aparece "inactive" o "dead", arráncalo con:

     ```
     sudo systemctl start ssh
     ```

   - Para que arranque siempre al iniciar Ubuntu:

     ```
     sudo systemctl enable ssh
     ```

3. **Comprobar el puerto 22**:

   ```
   sudo ss -tulpn | grep ssh
   ```

   Si está escuchando, deberías ver algo como `0.0.0.0:22`.

4. **Firewall (UFW)**
   Si tienes **ufw** activado en Ubuntu, abre el puerto 22:

   ```
   sudo ufw allow ssh
   sudo ufw reload
   ```

   ```
   jose@jose-VirtualBox:~$ sudo ss -tulpn | grep ssh
   tcp   LISTEN 0      4096         0.0.0.0:22        0.0.0.0:*    users:(("sshd"
   ,pid=11744,fd=3),("systemd",pid=1,fd=353))
   tcp   LISTEN 0      4096            [::]:22           [::]:*    users:(("sshd"
   ,pid=11744,fd=4),("systemd",pid=1,fd=359))
   jose@jose-VirtualBox:~$ sudo ufw allow ssh
   Reglas actualizadas
   Reglas actualizadas (v6)
   ```

5. **Probar conexión desde otra máquina**:

   ```
   ssh feval@192.168.1.45
   ```

4. Prueba de funcionamiento

Desde otra máquina o usando el mismo host (con cuidado):

```
ssh usuario@tu_ip -p 22
ssh feval@192.168.1.45 -p 22
```

Introduce varias contraseñas incorrectas.

```
┌──(kali㉿kali)-[~]
└─$ ssh jose@192.168.1.41 -p 22
The authenticity of host '192.168.1.41 (192.168.1.41)' can't be est
ablished.
ED25519 key fingerprint is SHA256:L6JYVwicEvLNP2QP4m2/3xTCCrhN6euTQ
QLvzdytaL8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])
? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.1.41' (ED25519) to the list of
known hosts.
jose@192.168.1.41's password:
Permission denied, please try again.
jose@192.168.1.41's password:
Permission denied, please try again.
jose@192.168.1.41's password:
jose@192.168.1.41: Permission denied (publickey,password).
```

Luego revisa si la IP fue bloqueada:

sudo fail2ban-client status sshd

Debería mostrar la IP bajo “Banned IP list”.

```
jose@jose-VirtualBox:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     3
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
   |- Currently banned: 1
   |- Total banned:     1
   `- Banned IP list:   192.168.1.42
```

Para desbloquear manualmente una IP:

sudo fail2ban-client set sshd unbanip 192.168.1.42

```
jose@jose-VirtualBox:~$ sudo fail2ban-client set sshd unbanip 192.168.1.42
1
jose@jose-VirtualBox:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     3
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
   |- Currently banned: 0
   |- Total banned:     1
   `- Banned IP list:
```

5. Extensiones útiles

- **Enviar notificaciones por correo** cuando se bloquea una IP (útil en servidores de producción).
- Crear filtros personalizados para otros servicios (ejemplo: Apache, Nginx, Postfix, Dovecot).
- Ajustar bantime a -1 para bloquear **permanentemente**.

Ejemplo de otra *jail* para proteger Apache:

```
[apache-auth]
enabled = true
port = http,https
logpath = /var/log/apache*/*error.log
maxretry = 5
```

6. Verificación de logs

Logs de Fail2Ban:

sudo tail -f /var/log/fail2ban.log

```
jose@jose-VirtualBox:~$ sudo tail -f /var/log/fail2ban.log
2025-10-01 09:06:50,630 fail2ban.filter         [8569]: INFO      findtime: 600
2025-10-01 09:06:50,630 fail2ban.actions        [8569]: INFO      banTime: 600
2025-10-01 09:06:50,630 fail2ban.filter         [8569]: INFO      encoding: UTF-8
2025-10-01 09:06:50,641 fail2ban.filtersystemd  [8569]: INFO    [sshd] Jail is in operation now (process new journal entries)
2025-10-01 09:06:50,647 fail2ban.jail           [8569]: INFO    Jail 'sshd' started
2025-10-01 09:27:58,245 fail2ban.filter         [8569]: INFO    [sshd] Found 192.168.1.42 - 2025-10-01 09:27:57
2025-10-01 09:28:08,225 fail2ban.filter         [8569]: INFO    [sshd] Found 192.168.1.42 - 2025-10-01 09:28:07
2025-10-01 09:28:15,072 fail2ban.filter         [8569]: INFO    [sshd] Found 192.168.1.42 - 2025-10-01 09:28:14
2025-10-01 09:28:15,361 fail2ban.actions        [8569]: NOTICE  [sshd] Ban 192.168.1.42
2025-10-01 09:30:33,422 fail2ban.actions        [8569]: NOTICE  [sshd] Unban 192.168.1.42
```

Resumen:

- Monitoreo de **logs**.
- Uso de **expresiones regulares** para detectar ataques.
- Gestión de **firewall automático** con Fail2Ban.
- Buenas prácticas de **hardening de servidores**.