

# Proteger mi Linux con fail2ban

León Ramos @fulvous  
@creadoresdigita

Levanta su servidor Linux en  
Internet




  
**3 doritos despues**  
(horas)

Los juackers ya tienen  
acceso a su servidor



# ¿Cómo?



```
graph LR; A[Detectar "ataque" en las Bitácoras del sistema (logs)] --> B[Bloquear la ip Con una regla iptables]; B --> C[Esperar un Tiempo y Desbloquear La ip];
```

Detectar "ataque" en las Bitácoras del sistema (logs)

Bloquear la ip  
Con una regla iptables

Esperar un  
Tiempo y  
Desbloquear  
La ip

# ¡¡fail2ban!!

- 2003
- Software Libre
- Python
- Progamadores
  - Cyril Jaquier
  - Arturo 'Buanzo' Busleiman
- Sitio
  - <http://fail2ban.org>
- Manual
  - [http://fail2ban.org/wiki/index.php/MANUAL\\_08](http://fail2ban.org/wiki/index.php/MANUAL_08)
- Wikipedia
  - <https://es.wikipedia.org/wiki/Fail2ban>

# Palabras clave

- **filter** = expresión regular que corresponde a un archivo log a revisar
- **action** = comandos que serán ejecutados según corresponda
- **jail** = combinación de un filtro y una o varias acciones

# Jugada a balón parado

## *Proteger ssh*

### 1) Instalar fail2ban

```
apt-get install fail2ban
```

### 2) Validar que arranque al inicio

```
systemctl is-enabled fail2ban
```

```
systemctl list-units-file | grep fail2ban
```

Los archivos `.local` sobre escriben a los `.conf`  
(excepto `paths-common.conf` que se sobreescribe con `paths-overrides.local`)

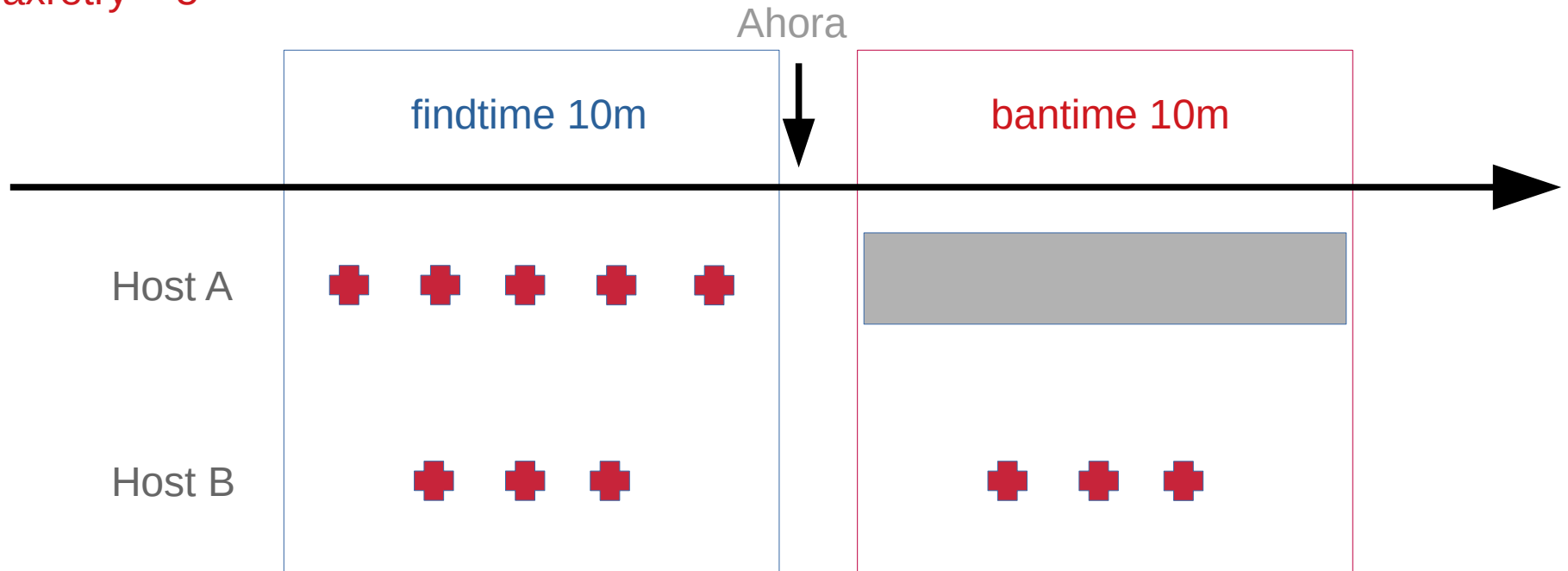
### Estructura de directorios

```
/etc/fail2ban# tree -L 1 -p
```

```
.
├── [drwxr-xr-x] action.d
├── [-rw-r--r--] fail2ban.conf
├── [drwxr-xr-x] fail2ban.d
├── [drwxr-xr-x] filter.d
├── [-rw-r--r--] jail.conf
├── [drwxr-xr-x] jail.d
├── [-rw-r--r--] paths-arch.conf
├── [-rw-r--r--] paths-common.conf
├── [-rw-r--r--] paths-debian.conf
└── [-rw-r--r--] paths-opensuse.conf
```

# bantime vs findtime

Maxretry = 5



# Configurar mi jail

## 1) /etc/fail2ban/jail.local

[DEFAULT]

bantime = 5m

findtime = 2m

maxretry = 5

#OPCIONAL

destemail = micorreo@dominio.com

sender = fail2ban@debian10test

mta = mail

Puedes descargar el archivo aquí:

<https://github.com/fulvous/fail2ban-tuto>

Necesario configurar envío de correo

<https://proyectoa.com/enviar-mail-con-postfix-en-linux-con-servidor-externo-gmail-o-cualquier-otro/>





# Configurar mi jail (cont)

**/etc/fail2ban/jail.local (cont)**

[sshd]

enable = true

port = ssh

logpath = %(sshd\_log)s → Log a revisar /var/log/auth.log

backend = %(sshd\_backend)s → systemd

# Comandos interesantes

- Ver estado del jail
  - `fail2ban-client status sshd`
  - `watch -n1 fail2ban-client status sshd`
- Ver bloqueo con iptables
  - `iptables -L -n`
- Desbloquear una ip
  - `fail2ban-client set sshd unbanip 192.168.1.1`
- Poner una ip en lista limpia (blanca)
  - `fail2ban-client set sshd addignoreip 192.168.1.1`

# Ejemplo de correo

[Fail2Ban] sshd: banned 192.168.15.100 from debian10test

Recibidos x



root <root@debian10test>

para



inglés



español

[Traducir mensaje](#)

[Desactivar para: inglés](#) x

Hi,

The IP 192.168.15.100 has just been banned by Fail2Ban after  
5 attempts against sshd.

Here is more information about 192.168.15.100 :

#

# ARIN WHOIS data and services are subject to the Terms of Use

# available at: <https://www.arin.net/resources/registry/whois/tou/>

#

# If you see inaccuracies in the results, please report at

# [https://www.arin.net/resources/registry/whois/inaccuracy\\_reporting/](https://www.arin.net/resources/registry/whois/inaccuracy_reporting/)

#

# Copyright 1997-2021, American Registry for Internet Numbers, Ltd.

#

# ¡Felices bloqueos!

- León Ramos
  - @fulvous
  - @creadoresdigita
  - creadoresdigitales.com
  - meganucleo.mx