

Fail2Ban

Setup

1. Update and install `apt update && apt upgrade -y && apt install -y fail2ban`
2. Start fail2ban and set it to auto start on boot `sudo systemctl start fail2ban && sudo systemctl enable fail2ban`
3. Make a local copy of the config file (why? because jail.conf get wiped after each update)
`sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local`
4. Open jail.local and setup stuff

Actions

Unbanning IP `fail2ban-client set YOUR_JAIL_NAME_HERE unbanip IP_ADDRESS`

Banning IP `fail2ban-client JAIL_NAME banip IP_ADDRESS`

Changing max retry attempts

1. Open file located at `etc/fail2ban/jail.local`
2. Add `maxretry = x` under `[sshd]`
3. Restart fail to ban `sudo systemctl restart fail2ban`

A good default

```
[sshd]
enabled = true
filter = sshd
maxretry = 3
findtime = 1h
bantime = 1y
port    = ssh
logpath = %(sshd_log)s
backend = %(sshd_backend)s
```

ignoreip = 125.253.46.252

Revision #2

Created 22 March 2025 09:30:08 by Conor

Updated 3 July 2026 23:02:04 by Conor