

Renforcement de la Sécurité avec Fail2Ban : Détection et Protection des Accès

SERIGNE KHADIM FAYE

IT Network Systeme Security

Cyber Security Enthusiast

fayekhadim96s@gmail.com

Fail2Ban



Gestion des Accès et Sécurisation des Services avec
Fail2Ban

SERIGNE KHADIM FAYE

XAM XAM DOU DOY!

Introduction

La sécurité des systèmes est une priorité essentielle pour prévenir les attaques et protéger les services critiques. L'une des menaces les plus courantes est l'attaque par force brute, qui consiste à essayer de deviner des identifiants de connexion en testant de nombreuses combinaisons.

Fail2Ban est un outil puissant permettant de surveiller les tentatives de connexion et de bloquer automatiquement les adresses IP suspectes.

Ce document couvre l'installation et la configuration de Fail2Ban pour protéger un serveur Debian, ainsi que l'intégration avec **Postfix** pour recevoir des alertes par email via **Gmail**.

1. Présentation de Fail2Ban

Fail2Ban est un logiciel de protection contre les attaques basées sur l'analyse des logs des services comme SSH, Apache, et bien d'autres. Il fonctionne en surveillant les fichiers journaux et en appliquant des règles pour bloquer les adresses IP malveillantes en modifiant les règles du pare-feu du système.

Principales fonctionnalités :

- Détection des tentatives de connexion infructueuses répétées
- Blocage automatique des adresses IP suspectes
- Personnalisation des règles de détection et d'action
- Envoi d'alertes par e-mail en cas de détection d'une attaque
- Etc.

Installation de Fail2Ban

Sur un serveur Debian, installons Fail2Ban avec :

```
sudo apt update
```

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

```
root@DebianBambafaye:~# uname -a
Linux DebianBambafaye 6.1.0-31-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.128-1 (2025-02-07) x86_64 GNU/Linux
root@DebianBambafaye:~# apt update
Hit:1 http://deb.debian.org/debian bookworm InRelease
Hit:2 http://security.debian.org/debian-security bookworm-security InRelease
Hit:3 http://deb.debian.org/debian bookworm-updates InRelease
Hit:4 https://repo.zabbix.com/zabbix/7.2/release/debian bookworm InRelease
Hit:5 https://repo.zabbix.com/zabbix-tools/debian-ubuntu bookworm InRelease
Hit:6 https://repo.zabbix.com/zabbix/7.2/stable/debian bookworm InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
60 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@DebianBambafaye:~# apt install fail2ban -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  python3-pyinotify python3-systemd whois
Suggested packages:
  mailx monit sqlite3 python-pyinotify-doc
The following NEW packages will be installed:
  fail2ban python3-pyinotify python3-systemd whois
0 upgraded, 4 newly installed, 0 to remove and 60 not upgraded.
Need to get 589 kB of archives.
After this operation, 2,901 kB of additional disk space will be used.
Get:1 http://deb.debian.org/debian bookworm/main amd64 fail2ban all 1.0.2-2 [451 kB]
Get:2 http://deb.debian.org/debian bookworm/main amd64 python3-pyinotify all 0.9.6-2 [27.4 kB]
Get:3 http://deb.debian.org/debian bookworm/main amd64 python3-systemd amd64 235-1+b2 [20.2 kB]
Get:4 http://deb.debian.org/debian bookworm/main amd64 whois all 5.4.0-2 [11.5 kB]

```

Autorisons le démarrage du service avec le démarrage du système, démarrons le service et vérifions son état.

```
sudo systemctl enable fail2ban
```

```
sudo systemctl start fail2ban
```

```
root@DebianBambafaye:~# systemctl enable fail2ban
Synchronizing state of fail2ban.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable fail2ban
root@DebianBambafaye:~# systemctl start fail2ban
root@DebianBambafaye:~# systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
   Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; preset: enabled)
   Active: active (running) since Fri 2025-03-28 18:01:22 EDT; 1min 33s ago
     Docs: man:fail2ban(1)
  Main PID: 2779 (fail2ban-server)
    Tasks: 5 (limit: 1056)
   Memory: 14.8M
      CPU: 167ms
  CGroup: /system.slice/fail2ban.service
          └─2779 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

Mar 28 18:01:22 DebianBambafaye systemd[1]: Started fail2ban.service - Fail2Ban Service.
Mar 28 18:01:22 DebianBambafaye fail2ban-server[2779]: 2025-03-28 18:01:22,794 fail2ban.configreader [2779]: WARNING 'a
Mar 28 18:01:23 DebianBambafaye fail2ban-server[2779]: Server ready

root@DebianBambafaye:~# ps auxw | grep [f]ail2ban
root      2779  0.0  2.4 400200 23220 ?        Ssl  18:01   0:00 /usr/bin/python3 /usr/bin/fail2ban-server -xf start
root@DebianBambafaye:~#
```

Configuration de Fail2Ban

Création et configuration d'une règle pour SSH

Nous allons créer une règle pour protéger le service SSH contre les tentatives de connexion par force brute.

Copions le fichier de configuration par défaut (conseillé, ou travaillé sur le dossier jail.d) :

`cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local` et éditons le fichier jail.local

```
root@DebianBambafaye:~# ls -l /etc/fail2ban/
total 64
drwxr-xr-x 2 root root 4096 Mar 28 18:01 action.d
-rw-r--r-- 1 root root 3017 Nov 9 2022 fail2ban.conf
drwxr-xr-x 2 root root 4096 Apr 21 2023 fail2ban.d
drwxr-xr-x 3 root root 4096 Mar 28 18:01 filter.d
-rw-r--r-- 1 root root 25607 Nov 9 2022 jail.conf
drwxr-xr-x 2 root root 4096 Mar 28 18:01 jail.d
-rw-r--r-- 1 root root 645 Nov 9 2022 paths-arch.conf
-rw-r--r-- 1 root root 2728 Nov 9 2022 paths-common.conf
-rw-r--r-- 1 root root 627 Nov 9 2022 paths-debian.conf
-rw-r--r-- 1 root root 738 Nov 9 2022 paths-opensuse.conf
root@DebianBambafaye:~# cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
root@DebianBambafaye:~# ls -l /etc/fail2ban/
total 92
drwxr-xr-x 2 root root 4096 Mar 28 18:01 action.d
-rw-r--r-- 1 root root 3017 Nov 9 2022 fail2ban.conf
drwxr-xr-x 2 root root 4096 Apr 21 2023 fail2ban.d
drwxr-xr-x 3 root root 4096 Mar 28 18:01 filter.d
-rw-r--r-- 1 root root 25607 Nov 9 2022 jail.conf
drwxr-xr-x 2 root root 4096 Mar 28 18:01 jail.d
-rw-r--r-- 1 root root 25607 Mar 28 18:12 jail.local
-rw-r--r-- 1 root root 645 Nov 9 2022 paths-arch.conf
-rw-r--r-- 1 root root 2728 Nov 9 2022 paths-common.conf
-rw-r--r-- 1 root root 627 Nov 9 2022 paths-debian.conf
-rw-r--r-- 1 root root 738 Nov 9 2022 paths-opensuse.conf
root@DebianBambafaye:~#
```

`vim /etc/fail2ban/jail.local`

```
70 #
71 # SSH servers Jail Conf Start =====
72
73 [sshd]
74 enabled = true
75 port = ssh
76 filter = sshd
77 logpath = /var/log/auth.log
78 maxretry = 3
79 bantime = 3600
80 findtime = 60
81 destemail = [REDACTED]@gmail.com
82 sender = [REDACTED]@gmail.com
83 mta = sendmail
84 action = %(action_mwl)s
85
86
87 # SSH Servers jail conf End =====
88
```

Explication de la regle [SSHD]

- *maxretry = 3* → Après **5 tentatives** échouées, l'IP est bannie.
- *bantime = 3600* → Bannissement pendant **1 heure**.
- *findtime = 60* → Si **3 tentatives d'accès échecs** en **1 minutes**, le bannissement s'applique pour **1H** de temps.
- *action = %(action_mwl)s* → Envoie un **mail** avec **les logs** en pièce jointe.
- *destemail* → L'e-mail qui recevra les alertes
sender → L'e-mail expéditeur (doit être le même que celui configuré dans Postfix)
- *mta* → *sendmail* car Postfix est installé

Configurer l'Envoi des Mails via Gmail

Fail2Ban utilise sendmail par défaut. Nous allons configurer Postfix pour envoyer les mails via Gmail.

Etape 1 : Installer Postfix et Mailutils

```
sudo apt update
```

```
sudo apt install postfix mailutils
```

Lors de l'installation, choisis :

- **Type de configuration** : "Site Internet".

```
oot@DebianBambafaye:~# sudo apt update
Hit:1 http://security.debian.org/debian-security bookworm-security InRelease
Hit:2 http://deb.debian.org/debian bookworm InRelease
Hit:3 http://deb.debian.org/debian bookworm-updates InRelease
Hit:4 https://repo.zabbix.com/zabbix/7.2/release/debian bookworm InRelease
Hit:5 https://repo.zabbix.com/zabbix-tools/debian-ubuntu bookworm InRelease
Hit:6 https://repo.zabbix.com/zabbix/7.2/stable/debian bookworm InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
8 packages can be upgraded. Run 'apt list --upgradable' to see them.
oot@DebianBambafaye:~# sudo apt install postfix mailutils
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  gpg-wks-client libgsasl-common guile-3.0-libs libfribidi0 libgc1 libgsasl18 libgssglue1 libidn12
Suggested packages:
  mailutils-mh mailutils-doc procmail postfix-mysql postfix-pgsql postfix-ldap postfix-imap4 postfix-man
  postfix-mta-sts-resolver ufw postfix-doc
The following NEW packages will be installed:
  gpg-wks-client libgsasl-common guile-3.0-libs libfribidi0 libgc1 libgsasl18 libgssglue1 libidn12
0 upgraded, 14 newly installed, 0 to remove and 58 not upgraded.
Need to get 13.5 MB of archives.
After this operation, 75.2 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Hit:1 http://deb.debian.org/debian bookworm/main amd64 postfix amd64 3.7.11-0+deb
Hit:2 http://deb.debian.org/debian bookworm/main amd64 gpg-wks-client all 2.2.0-1 f
```

- **Nom du serveur mail : ton_domaine.com (ou laisse par défaut).**

```

Postfix Configuration
Please select the mail server configuration type that best meets your needs.

No configuration:
Should be chosen to leave the current configuration unchanged.
Internet site:
Mail is sent and received directly using SMTP.
Internet with smarthost:
Mail is received directly using SMTP or by running a utility such
as fetchmail. Outgoing mail is sent using a smarthost.
Satellite system:
All mail is sent to another machine, called a 'smarthost', for
delivery.
Local only:
The only delivered mail is the mail for local users. There is no
network.

General mail configuration type:

No configuration
Internet Site
Internet with smarthost
Satellite system
Local only

<Ok>          <Cancel>

```

```

Postfix Configuration
The 'mail name' is the domain name used to 'qualify' ALL mail addresses without a domain name. This includes mail to and from <root@machine>
machine send out mail from root@example.org unless root@example.org has told you to.

This name will also be used by other programs. It should be the single, fully qualified domain name (FQDN).

Thus, if a mail address on the local host is foo@example.org, the correct value for this option would be example.org.

System mail name:
DebianBambafaye.localdomain

<Ok>          <Cancel>

```

Étape 2 : Configurer Postfix pour Utiliser Gmail

Éditons le fichier de configuration : `vim /etc/postfix/main.cf`

```

6 smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination
7 myhostname = DebianBambafaye.localdomain
8 alias_maps = hash:/etc/aliases
9 alias_database = hash:/etc/aliases
0 myorigin = /etc/mailname
1 mydestination = $myhostname, DebianBambafaye.localdomain, localhost.localdomain, , localhost
2 #relayhost =
3 mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
4 mailbox_size_limit = 0
5 recipient_delimiter = +
6 inet_interfaces = all
7 inet_protocols = all
8
9 # Config SMTP google =====
0 relayhost = [smtp.gmail.com]:587
1 smtp_use_tls = yes
2 smtp_sasl_auth_enable = yes
3 smtp_sasl_security_options = noanonymous
4 smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
5 smtp_tls_CAfile = /etc/ssl/certs/ca-certificates.crt
6
7 # End config SMTP google =====

```

Créons un fichier d'authentification : `nano /etc/postfix/sasl_passwd`

```
smtp.gmail.com]:587 [redacted]@gmail.com [redacted] \nlnr
```

Appliquons les permissions et mettons à jour Postfix :

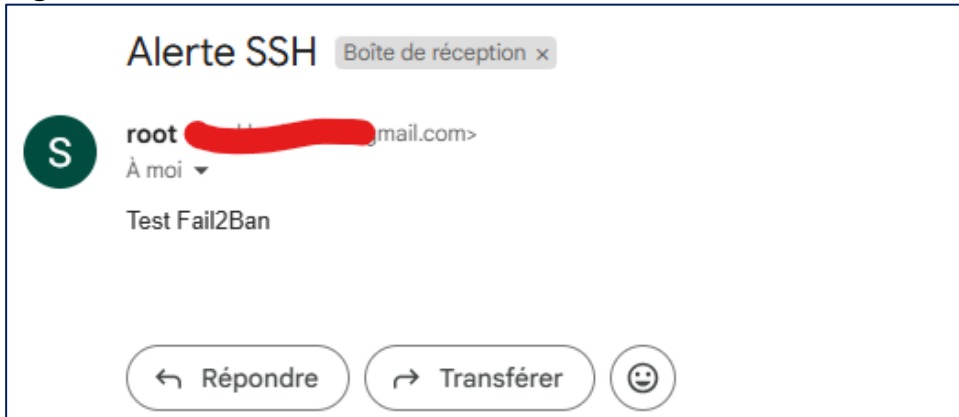
```

pot@DebianBambafaye:~# nano /etc/postfix/sasl_passwd
pot@DebianBambafaye:~# sudo chmod 600 /etc/postfix/sasl_passwd
pot@DebianBambafaye:~# sudo postmap /etc/postfix/sasl_passwd
pot@DebianBambafaye:~# sudo systemctl restart postfix
pot@DebianBambafaye:~# echo "Test Fail2Ban" | mail -s "Alerte SSH" [redacted].com

```

Testons l'envoi d'un mail :

La configuration est OK.



Relançons la configuration de fail2ban et vérifions son status

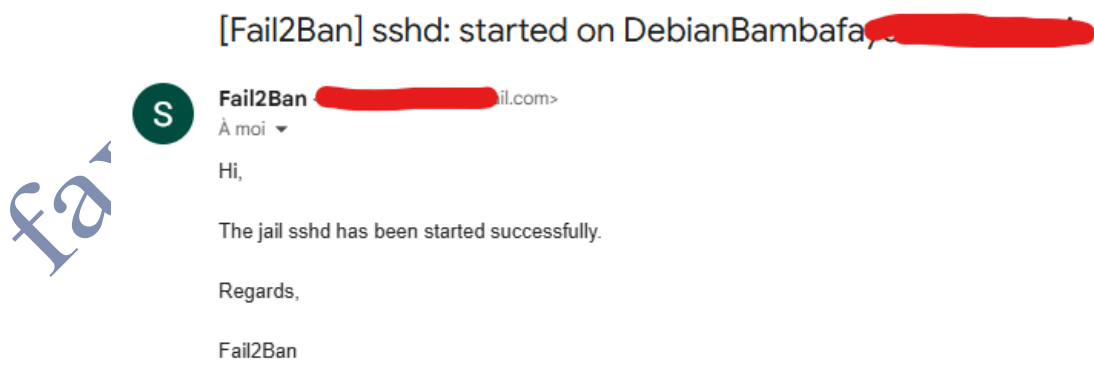
sudo systemctl restart fail2ban , sudo fail2ban-client status sshd

```
DebianBambafaye:~# systemctl status fail2ban
fail2ban.service - Fail2Ban Service
  Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; preset: enabled)
  Active: active (running) since Fri 2025-03-28 19:22:30 EDT; 10s ago
  Docs: man:fail2ban(1)
  Main PID: 5444 (fail2ban-server)
  Tasks: 5 (limit: 1056)
  Memory: 16.2M
  CPU: 113ms
  CGroup: /system.slice/fail2ban.service
          └─5444 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

Mar 28 19:22:30 DebianBambafaye systemd[1]: Started fail2ban.service - Fail2Ban Service.
Mar 28 19:22:31 DebianBambafaye fail2ban-server[5444]: 2025-03-28 19:22:31,005 fail2ban.config
Mar 28 19:22:31 DebianBambafaye fail2ban-server[5444]: Server ready

lines 1-14/14 (END)
```

D'ailleurs même, juste le fait de redémarrer le service, je reçois aussi une notification sur ma boîte mail !



À présent, passons sur notre machine attaquante pour simuler une attaque par brute force avec Hydra et vérifier si Fail2Ban détecte et bloque l'attaque comme prévu

Lançons l'attaque et observons les logs d'alertes

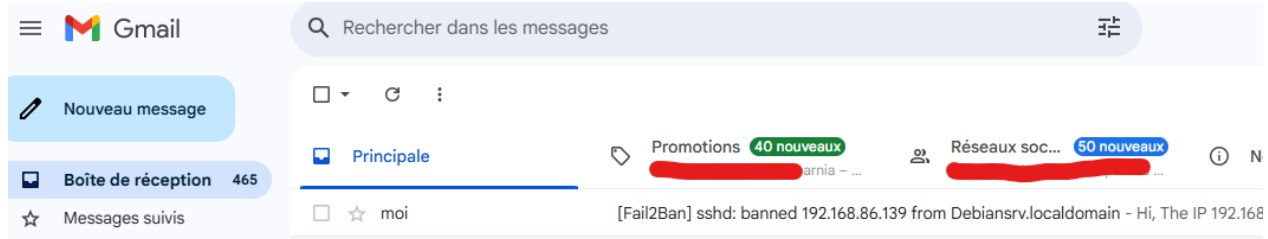
```
kali@kali)~$ sudo hydra -s 22 -l root -P /home/kali/Downloads/rockyou.txt [redacted] 9.135 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-28 20:02:36
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a pr
[DATA] max 64 tasks per 1 server, overall 64 tasks, 14344398 login tries (l:1/p:14344398), ~22413
[DATA] attacking ssh://[redacted]:22/
[ATTEMPT] target [redacted] login "root" - pass "123456" - 1 of 14344398 [child 0] (0/0)
[ATTEMPT] target [redacted] login "root" - pass "12345" - 2 of 14344398 [child 1] (0/0)
[ATTEMPT] target [redacted] login "root" - pass "123456789" - 3 of 14344398 [child 2] (0/0)
[ATTEMPT] target [redacted] login "root" - pass "password" - 4 of 14344398 [child 3] (0/0)
[ATTEMPT] target [redacted] login "root" - pass "iloveyou" - 5 of 14344398 [child 4] (0/0)
[ATTEMPT] target [redacted] login "root" - pass "princess" - 6 of 14344398 [child 5] (0/0)
[ATTEMPT] target [redacted] login "root" - pass "1234567" - 7 of 14344398 [child 6] (0/0)
[ATTEMPT] target [redacted] login "root" - pass "rockyou" - 8 of 14344398 [child 7] (0/0)
[ATTEMPT] target [redacted] login "root" - pass "12345678" - 9 of 14344398 [child 8] (0/0)
[ATTEMPT] target [redacted] login "root" - pass "abc123" - 10 of 14344398 [child 9] (0/0)
```

En vérifiant le fichier log, on voit que l'ip de l'attaquant est bloqué conformément à la règle mise en place.

```
root@DebianSRV:~# tail -T /var/log/fail2ban.log
2025-03-29 12:46:47,081 fail2ban.actions [7313]: NOTICE [sshd] 192.168.8
6.139 already banned
2025-03-29 12:46:47,081 fail2ban.actions [7313]: NOTICE [sshd] 192.168.8
6.139 already banned
2025-03-29 12:46:47,081 fail2ban.actions [7313]: NOTICE [sshd] 192.168.8
6.139 already banned
2025-03-29 12:46:47,081 fail2ban.actions [7313]: NOTICE [sshd] 192.168.8
6.139 already banned
2025-03-29 12:46:47,081 fail2ban.actions [7313]: NOTICE [sshd] 192.168.8
6.139 already banned
2025-03-29 12:46:47,081 fail2ban.actions [7313]: NOTICE [sshd] 192.168.8
6.139 already banned
2025-03-29 12:46:47,082 fail2ban.actions [7313]: NOTICE [sshd] 192.168.8
6.139 already banned
2025-03-29 12:46:47,082 fail2ban.actions [7313]: NOTICE [sshd] 192.168.8
6.139 already banned
2025-03-29 12:46:47,082 fail2ban.actions [7313]: NOTICE [sshd] 192.168.8
6.139 already banned
```

```
root@DebianSRV:~# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| - Currently failed: 1
| - Total failed: 44
| - File list: /var/log/auth.log
- Actions
| - Currently banned: 1
| - Total banned: 1
| - Banned IP list: [redacted] 6.139
root@DebianSRV:~#
```

Et nous recevons automatiquement une notification dans notre boîte mail.



[Fail2Ban] sshd: banned 192.168.86.139 from Debiansrv.localdomain - Hi, The IP 192.168.86.139 has just been banned by Fail2Ban after 3 attempts against sshd.

Hi,

The IP 192.168.86.139 has just been banned by Fail2Ban after 3 attempts against sshd.

Here is more information about 192.168.86.139 :

```
#
# 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/
#
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#

NetRange: 192.168.0.0 - 192.168.255.255
CIDR: 192.168.0/16
NetName: PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED
NetHandle: NET-192-168-0-0-1
Parent: NET192 (NET-192-0-0-0-0)
NetType: IANA Special Use
OriginAS:
Organization: Internet Assigned Numbers Authority (IANA)
RegDate: 1994-03-15
```

Et si l'attaquant tente encore l'attaque, il sera toujours bloqué et ne sera débloquenté qu'après les 1h de temps de bantime.

[ERROR] all children were disabled due to too many connection errors

On ne peut plus continuer car les connexions sont rejetées par le serveur.

```
DATA] attacking ssh://192.168.86.133:22/
ERROR] could not connect to ssh://192.168.86.133:22/ : connection refused
(bambafaye@kali)~$
```

```
RE-ATTEMPT] target 192.168.86.133 - login "root" - pass "superman" - 52 of 14344398 [child 0] (0/0)
ERROR] all children were disabled due to too many connection errors
) of 1 target completed, 0 valid password found
INFO] Writing restore file because 2 server scans could not be completed
ERROR] 1 target was disabled because of too many errors
ERROR] 1 targets did not complete
hydra (https://github.com/vanhauser-thc/thc-hydra) at 2025-03-29 12:48:45
```

Note : Pour garantir une protection optimale contre les attaques par force brute, il est essentiel d'affiner la configuration du jail SSH dans Fail2Ban. Des paramètres comme maxretry (nombre de tentatives avant bannissement), bantime (durée du bannissement) et findtime (fenêtre de détection) doivent être ajustés selon le niveau de sécurité souhaité.

En conclusion, Fail2Ban s'avère être une solution efficace pour atténuer les attaques par force brute en bloquant automatiquement les adresses IP suspectes. Cependant, pour renforcer davantage la sécurité, il est recommandé de désactiver l'authentification par mot de passe et d'opter pour un système basé sur des clés SSH. De plus, modifier le port par défaut du service SSH et restreindre les accès aux seules adresses IP autorisées ajoutent une couche de protection supplémentaire.

Toutefois, il est important de noter que le simple blocage d'une IP peut être inefficace face à des attaquants utilisant des méthodes avancées, telles que le pivoting à travers des machines compromises. Une approche de défense en profondeur, combinant pare-feu, segmentation réseau et surveillance continue, est donc essentielle pour une protection robuste et durable.

fayekhadim965@gmail.com