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

SERIGNE KHADIM FAYE
IT Network Systeme Security
Cyber Security Enthusiast
fayekhadim96s@gmail.com

Gestion des Accès et Sécurisation des Services avec Fail2Ban

SERIGNE KHADIM FAYE

XAM XAM DOU DOY!

Renforcement de la Sécurité avec Fail2Ban

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]
```

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 =                    @gmail.com
82 sender =                       gmail.com
83 mta = sendmail
84 action = %(action_mwl)s
85
86
87 # SSH Servers jail conf End ===================================
```

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

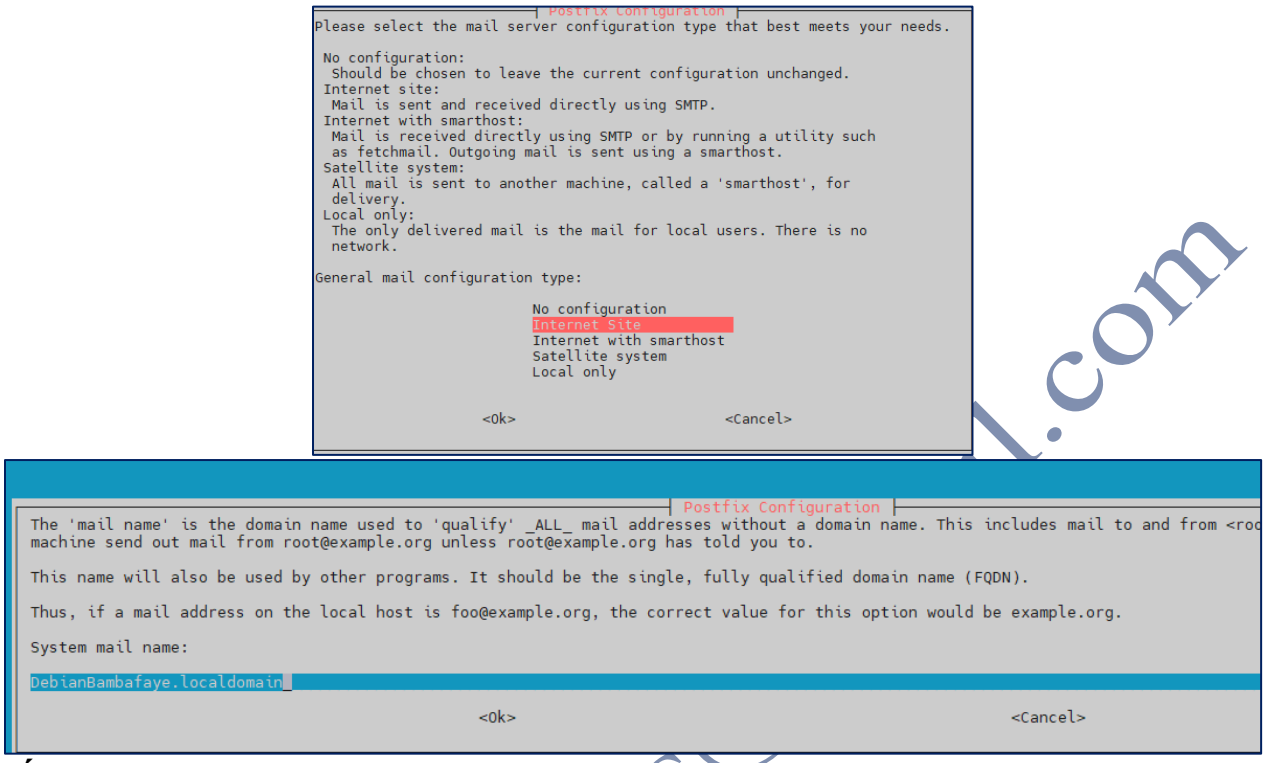
sudo apt install postfix mailutils

Lors de l'installation, choisis :

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

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

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



Étape 2 : Configurer Postfix pour Utiliser Gmail

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

```
smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination
myhostname = DebianBambafaye.localdomain
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = $myhostname, DebianBambafaye.localdomain, localhost.localdomain, , localhost
#relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = all

# Config SMTP google ======================
relayhost = [smtp.gmail.com]:587
smtp_use_tls = yes
smtp_sasl_auth_enable = yes
smtp_sasl_security_options = noanonymous
smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
smtp_tls_CAfile = /etc/ssl/certs/ca-certificates.crt

# End config SMTP google ======================
```

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

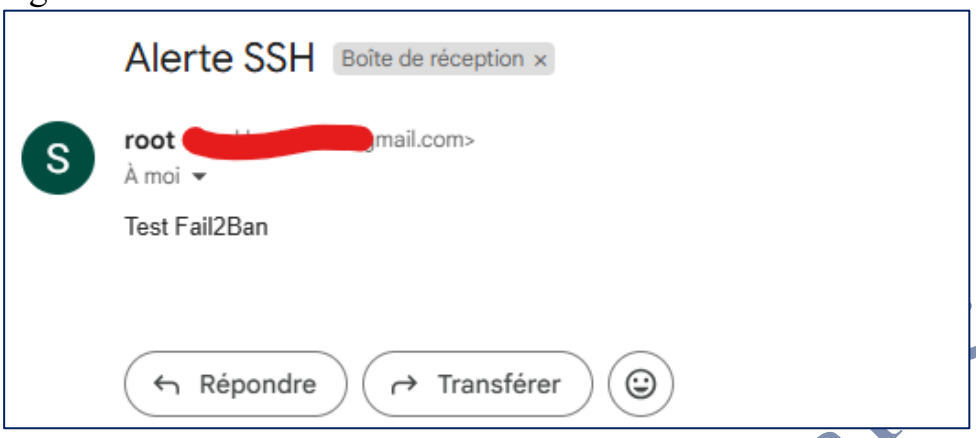
```
[smtp.gmail.com]:587 [redacted]@gmail.com [redacted]
```

Appliquons les permissions et mettons à jour Postfix :

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

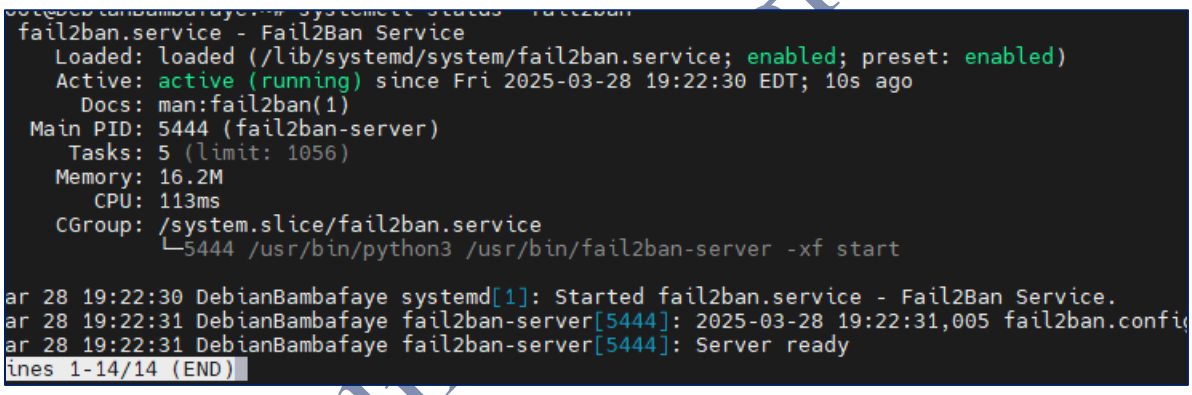
Testons l'envoi d'un mail :

La configuration est OK.

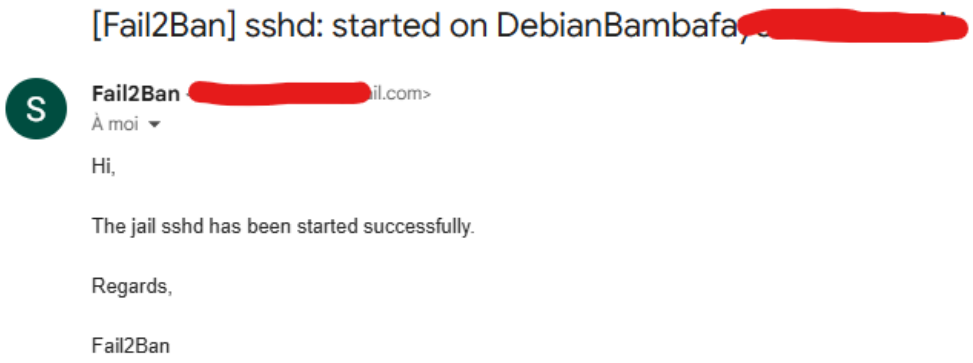


Relançons la configuration de fail2ban et vérifions son status

sudo systemctl restart fail2ban , sudo fail2ban-client status sshd

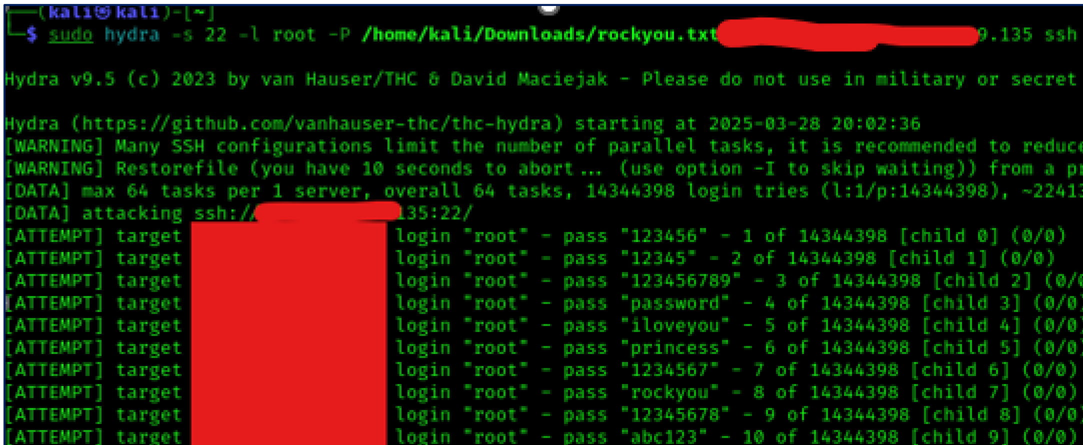


D'ailleurs même, juste le fait de redémarrer le service, je reçois aussi une notification sur ma boite mail !

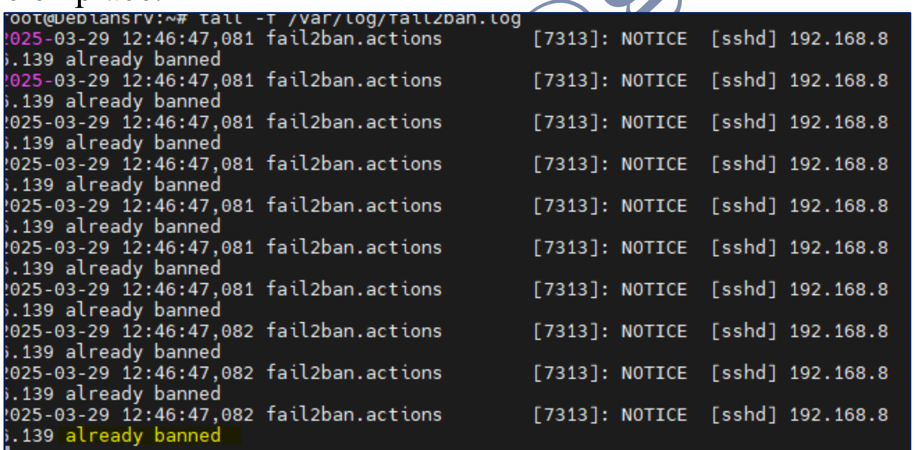


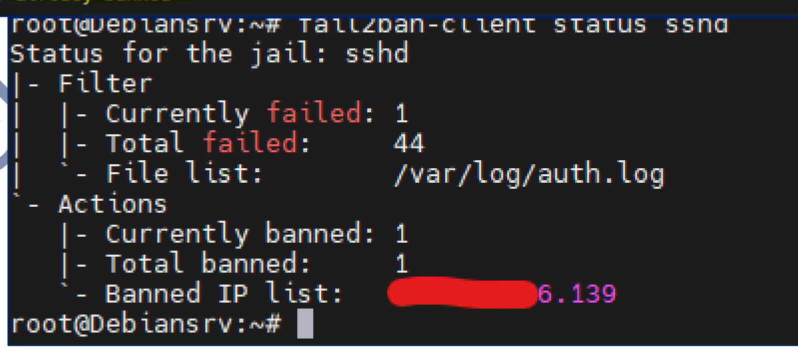
À présent, passons sur notre machine attaquante pour simuler une attaque par brute force avec Hydra et vérifier si Fail2Ban détecte et bloque l'attaque comme prévu

Lançons l'attaque et observons les logs d'alertes

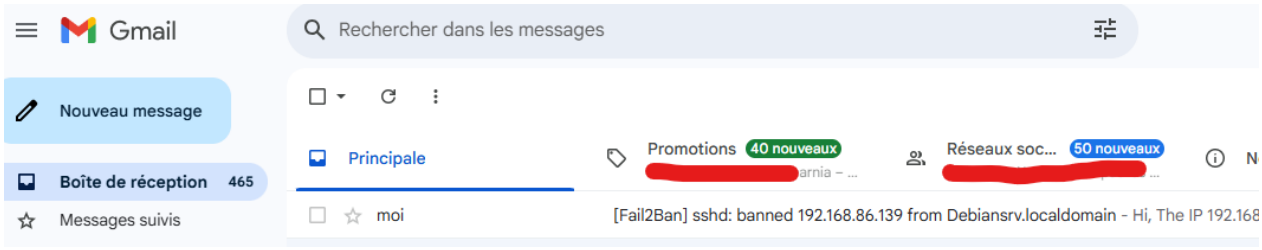


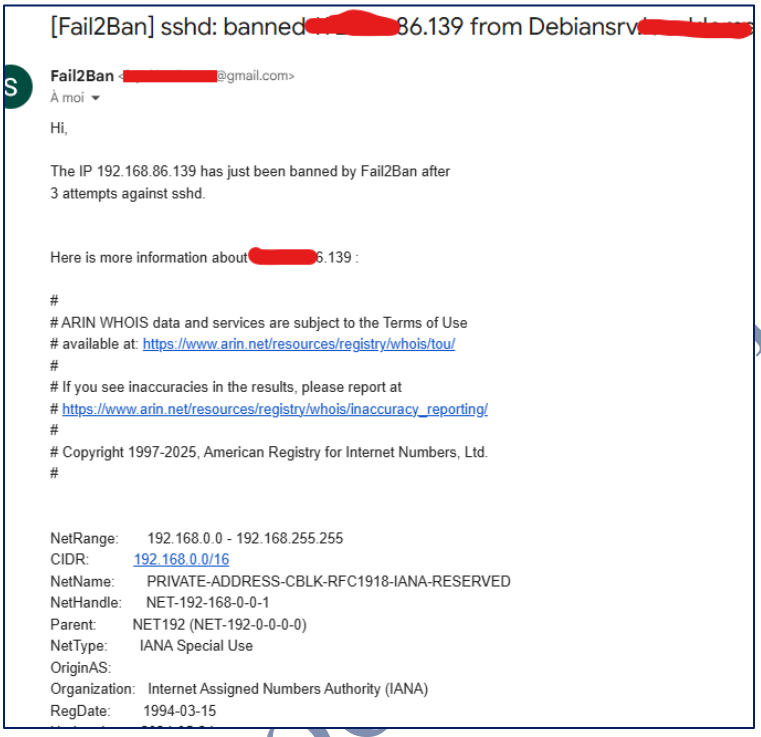
En vérifiant le fichier log, on voit que l'ip de l'attaquant est bloqué conformément à al règle mise en place.





Et nous recevons automatiquement une notification dans notre boit mail.

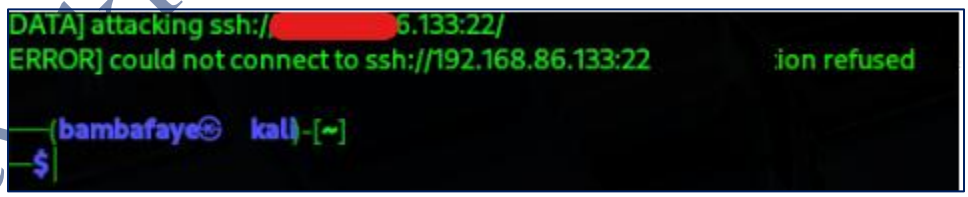


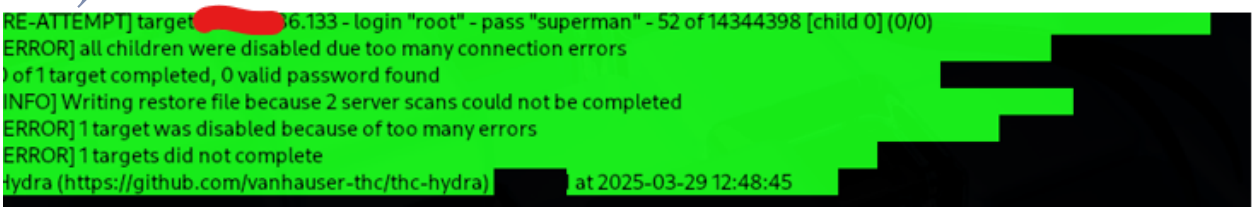


Et si l'attaquant tente encore l'attaque, il sera toujours bloqué et ne sera débloqué qu'après les 1h de temps de bantime.

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

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





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.