Installation de fail2ban sur le service vsftpd

Table des matières

Présentation :

Fail2ban est un service qui va ralentir les attaques par bruteforce en bannissant les adresses IP de l'attaquant, mais ne va pas empêcher pour autant ses attaques

Documentation technique :

On commence par mettre à jour le système et installons les différents services (fail2ban, iptables et vsftpd)iptables va servir de pare-feu pour vraiment bloquer les adresses IP contrairement à fail2ban qui va juste dire qu'il faut bannir cette adresse et non la bloquer.

```
root@Fail2ban:~# apt update && apt upgrade -y && apt install fail2ban iptables vsftpd
```

Etant donné qu'on ne peut pas se connecter en root sur le ftp, on va créer un utilisateur en faisant :

```
adduser admin
```

Dans vsftpd.conf on va passer 'listen = NO' en 'YES' et listen_ipv6 en 'NO' et on va également décommenter cette ligne, car de base les logs ne sont pas activé et fail2ban en a besoin pour fonctionner correctement.Après, enregistrer le fichier et redémarrer les services

```
# You may override where the log file goes if you like. The default is shown
# below.
#xferlog_file=/var/log/vsftpd.log
```

```
root@Fail2ban:~# systemctl restart fail2ban.service vsftpd.service
```

Documentation utilisateur :

On va maintenant, créer un fichier où l'on appellera avec le nom du service, dans ce cas on le fera avec vsftpd et mettrons en extension '.conf'

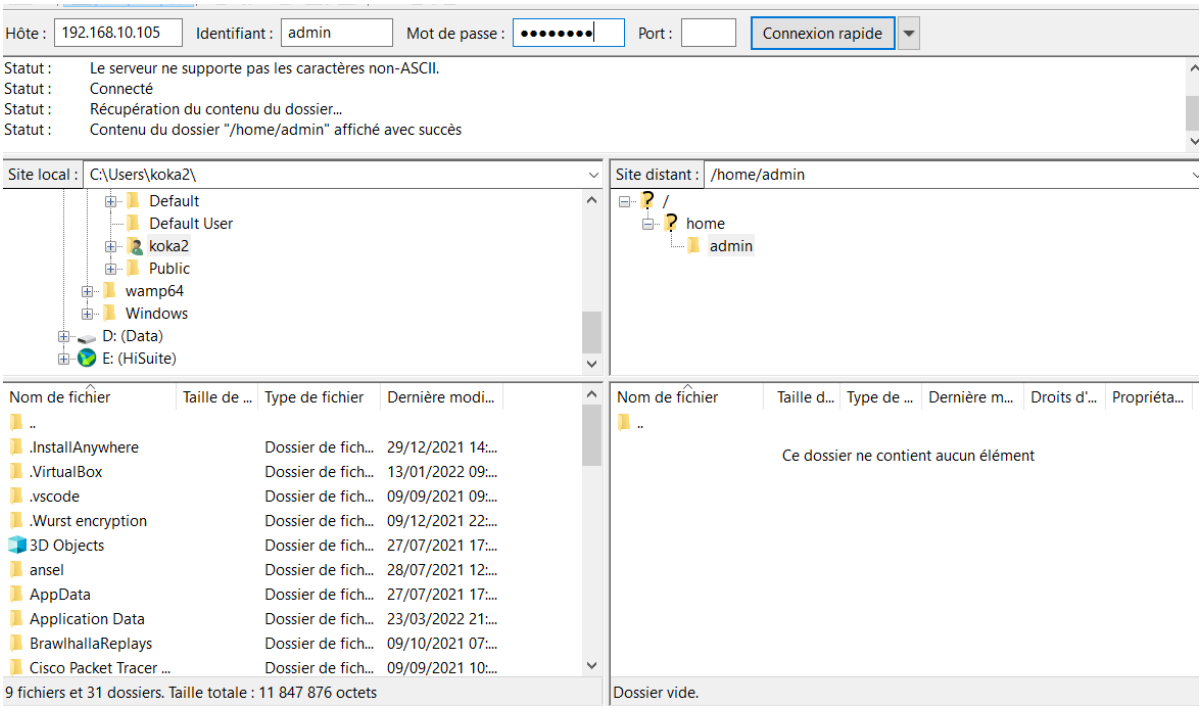
```
root@Fail2ban:~# nano /etc/fail2ban/jail.d/vsftpd.conf
```

Dans ce fichier il faut écrire ces lignes, à ajuster selon votre envie pour les 3 derniers paramètres

```
[vsftpd]
enabled = true
port = ftp,ftp-data,ftps,ftps-data
logpath = /var/log/vsftpd.log
maxretry = 2
bantime = 1m
findtime = 1h
```

Test :

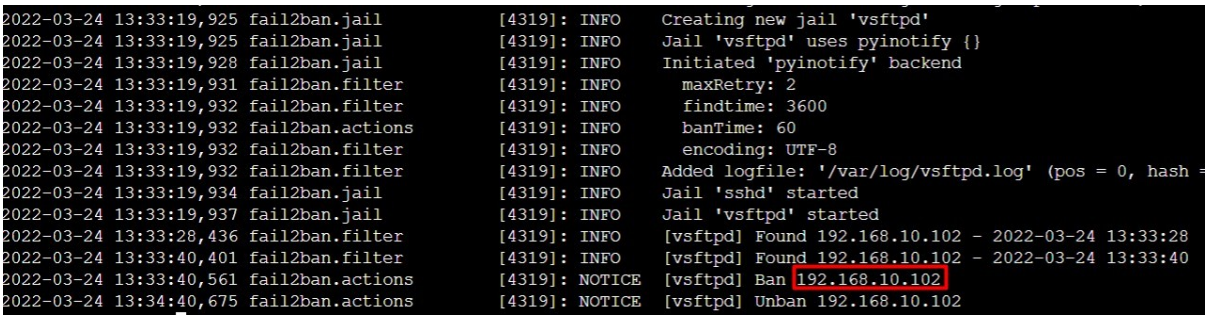
On voit que mon compte fonctionne quand je me connecte à l'aide de FileZilla, maintenant je vais faire exprès de me tromper de mot de passe



Allons afficher les logs de fail2ban à l'aide de la commande :

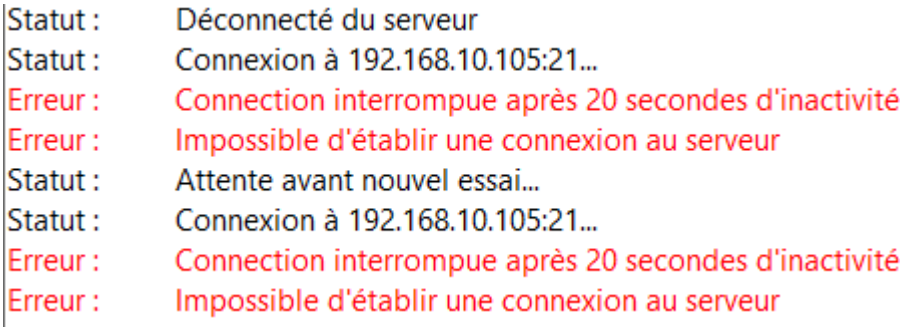
```
cat /var/log/fail2ban.log
```

On voit donc que mon ip s’est bien fait bannir puis débannir une minute après.



```
2022-03-24 13:33:19,925 fail2ban.jail           [4319]: INFO    Creating new jail 'vsftpd'
2022-03-24 13:33:19,925 fail2ban.jail           [4319]: INFO    Jail 'vsftpd' uses pyinotify {}
2022-03-24 13:33:19,928 fail2ban.jail           [4319]: INFO    Initiated 'pyinotify' backend
2022-03-24 13:33:19,931 fail2ban.filter         [4319]: INFO      maxRetry: 2
2022-03-24 13:33:19,932 fail2ban.filter         [4319]: INFO      findtime: 3600
2022-03-24 13:33:19,932 fail2ban.actions        [4319]: INFO      banTime: 60
2022-03-24 13:33:19,932 fail2ban.filter         [4319]: INFO      encoding: UTF-8
2022-03-24 13:33:19,932 fail2ban.filter         [4319]: INFO    Added logfile: '/var/log/vsftpd.log' (pos = 0, hash =
2022-03-24 13:33:19,934 fail2ban.jail           [4319]: INFO    Jail 'sshd' started
2022-03-24 13:33:19,937 fail2ban.jail           [4319]: INFO    Jail 'vsftpd' started
2022-03-24 13:33:28,436 fail2ban.filter         [4319]: INFO    [vsftpd] Found 192.168.10.102 - 2022-03-24 13:33:28
2022-03-24 13:33:40,401 fail2ban.filter         [4319]: INFO    [vsftpd] Found 192.168.10.102 - 2022-03-24 13:33:40
2022-03-24 13:33:40,561 fail2ban.actions        [4319]: NOTICE  [vsftpd] Ban 192.168.10.102
2022-03-24 13:34:40,675 fail2ban.actions        [4319]: NOTICE  [vsftpd] Unban 192.168.10.102
```

Sur FileZilla on peut également constater que je me suis fait bannir en regardant les statuts de connexions et les erreurs.



```
Statut :    Déconnecté du serveur
Statut :    Connexion à 192.168.10.105:21...
Erreur :    Connection interrompue après 20 secondes d'inactivité
Erreur :    Impossible d'établir une connexion au serveur
Statut :    Attente avant nouvel essai...
Statut :    Connexion à 192.168.10.105:21...
Erreur :    Connection interrompue après 20 secondes d'inactivité
Erreur :    Impossible d'établir une connexion au serveur
```