**Tuto Fail2ban**

**1)SSH**

Fail2ban est un Framework de prévention contre les intrusions, écrit en Python.

Afin d’éviter les attaques par brute force on peut paramétrer le ssh en ajoutant la configuration [sshd] sur le fichier de configuration de fail2ban (**cd /etc/fali2ban/**). Pour accéder au fichier j’ai utilisé la commande nano : **nano jail.local**

On peut ajouter les paramètres suivants :

Enable = true

Port = ssh

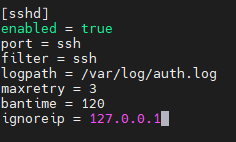
Filter = sshd

Logpath = /var/log/auth.log

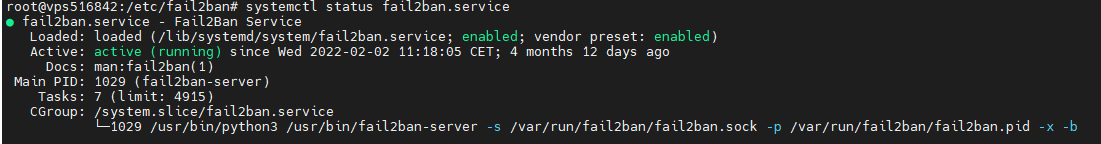
Maxretry = 3

Bantime = 120

Ignoreip = 127.0.0.1



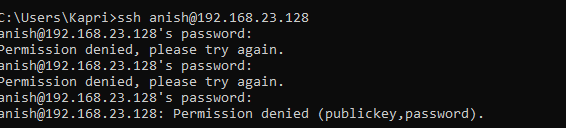
On doit redémarrer fail2ban avec la commande suivante : **systemctl restart fail2ban.service** et on va vérifier s'il est activé ou pas avec la commande : **systemctl status fail2ban.service**



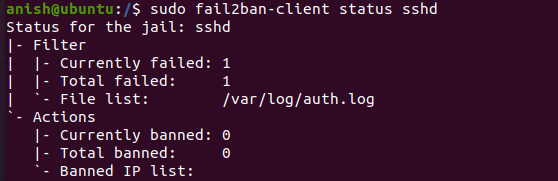
Puis on sauvegarde le fichier. Après cela on peut essayer de se connecter au ssh en mettant 3 fois le mauvais pot de passe et on sera banni pendant le temps paramétré sur le fichier de configuration.

Pour vérifier s'il y a eu des ip banni on peut taper la commande suivante : **fail2ban-client status sshd**

On peut aussi bannir des ip manuellement avec la commande : **sudo fail2ban-client set sshd banip (ip)**



Après trois tentatives j’avais plus l’accès au ssh.

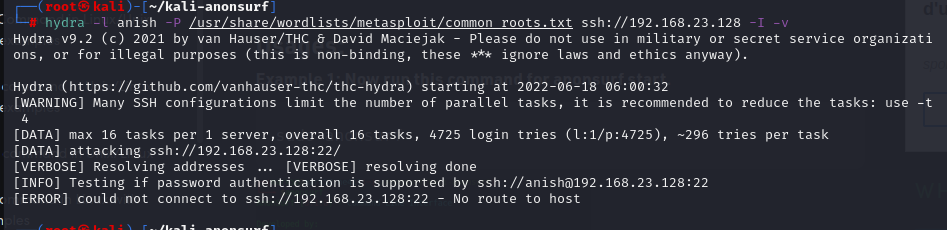


Et on remarque qu’il y a eu une tentative ratée.

**2)Démonstration avec une attaque.**

Hydra est un outil d’attaque de mot de passe (brute force) sur kali.

J’ai utilisé Hydra afin de faire une attaque sur mon serveur ssh.



J’ai utilisé la commande suivante : **hydra –l root –P /usr/share/wordlists/metasploit/common\_roots.txt ssh://(ip du serveur) -I –v**