FAIL2BAN/Patator

Fail2ban (et serveur ssh)

Fail2ban : est une application qui a pour objectif d'éviter de surcharger les logs du système avec des milliers de tentatives de connexion et de limiter la portée des attaques répétées provenant d'une même machine, qui sont généralement des attaques par force brute lancées par des robots.

IL analyse les logs ce qui permet de bannir les IP au bout d'un certain nombre de tentatives ce qui limitera le remplissage des logs et l'utilisation de la bande passante. Ceci va également rendre les attaques par force brute ou par dictionnaire beaucoup plus longues.

Installation de fail2ban : #sudo apt-get update (mets à jour la base de données de mes paquets) #sudo apt install fail2ban (Installe les paquets de fail2ban) #systemctl start fail2ban (lance le service fail2ban) #systemctl enable fail2ban (active le #systemctl status fail2ban

Aide pour installer Fail2ban : https://doc.ubuntu-fr.org/fail2ban

Installer Fail2ban :

```
sudo apt install Fail2ban
```

Lancer le service Fail2ban:

```
systemctl start fail2ban
```

Crée le démarrage automatique :

```
systemctl enable fail2ban
```

Contrôler la bonne installation :

```
systemctl status fail2ban
```

Configuration :

[...]

OpenSSH : est un ensemble d'outils informatiques libres permettant des communications sécurisées sur un réseau informatique en utilisant le protocole SSH.

Installation du serveur sshd :

```
sudo apt-get update
sudo apt-get install openssh-server
```

```
systemctl start sshd
sudo systemctl status sshd
```

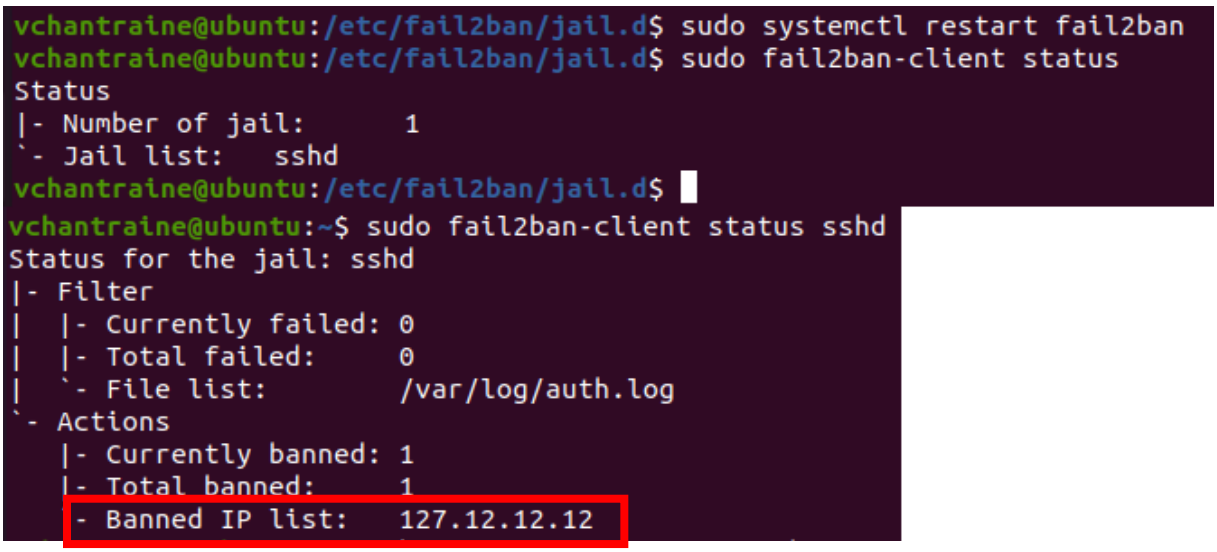
Relancez la configuration :

```
sudo systemctl restart fail2ban
```

Vérifier si les prisons correctement lancées :

```
sudo fail2ban-client status
```

Le résultat doit être (l'adresse IP 127.12.12.12 s'est fait bannir) :



Patator (attaque par brutes forces)

Maintenant nous allons tester notre serveur avec des attaques par brutes forces grâces à Patator

Patator : est un script python permettant à l'aide d'un dictionnaire/wordlist de lancer des attaques de type brute force (tester tous les mots de passe d'un dictionnaire pour trouver le bon mot de passe)

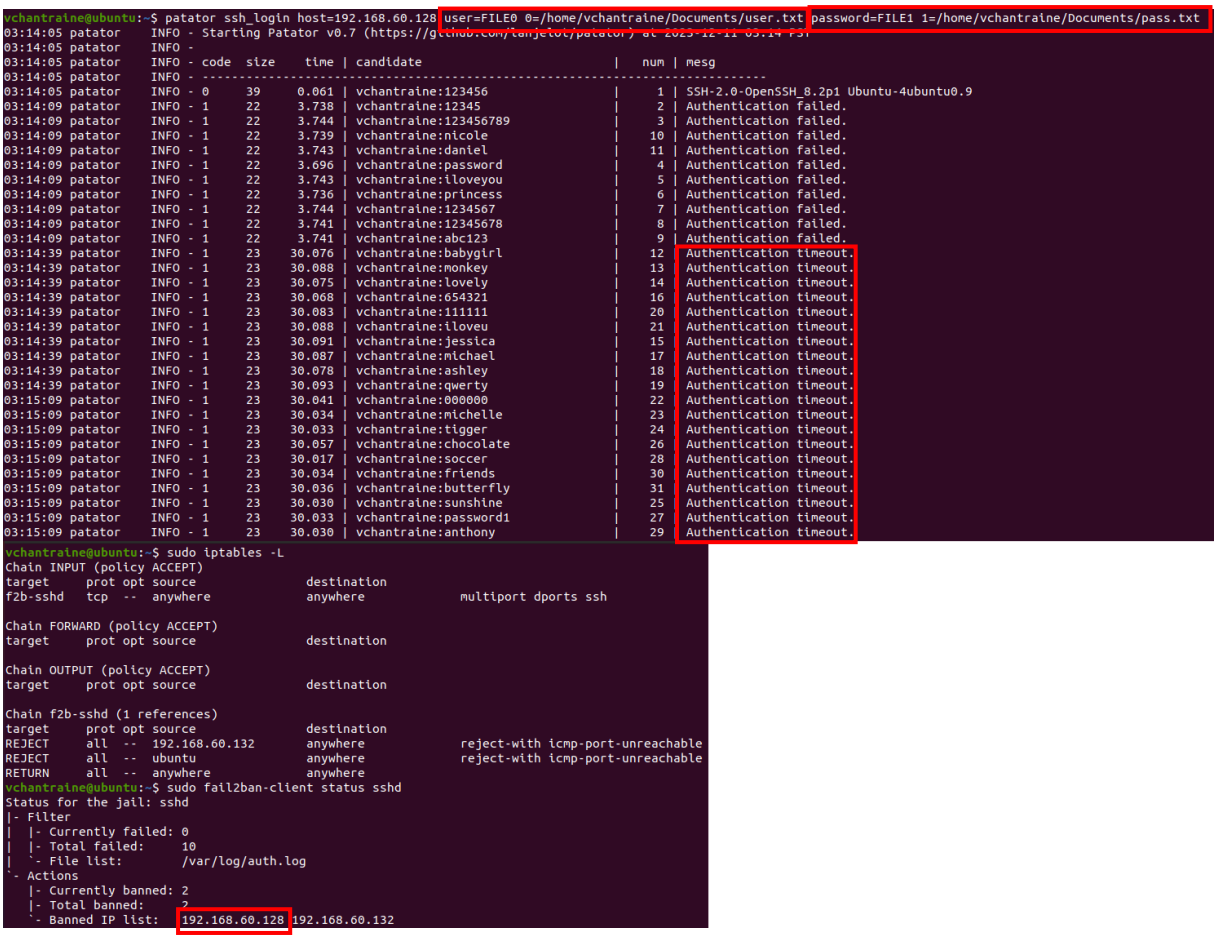
Installer patator :

```
sudo apt install patator
```

Pour effectuer cette attaque nous allons cloner notre machine virtuelle pour pouvoir l'attaquer (adresse IP différente).

Fichier user.txt et pass.txt contenant les noms d'utilisateur et les mots de passe.

Le résultat coter attaquant prouve le bannissement avec les authentication timeout. Prouvant qu'il n'est plus possible de réaliser d'autres tentatives de connexions ssh.



Est le résultat du côté défenseur où l'on peut observer l'adresse IP de l'attaquant banni.