

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) :

```
vchantraine@ubuntu:/etc/fail2ban/jail.d$ sudo systemctl restart fail2ban
vchantraine@ubuntu:/etc/fail2ban/jail.d$ sudo fail2ban-client status
Status
|- Number of jail:      1
`- Jail list:  sshd
vchantraine@ubuntu:/etc/fail2ban/jail.d$ 
vchantraine@ubuntu:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed:    0
| `-- File list:      /var/log/auth.log
`- Actions
   |- Currently banned: 1
   |- Total banned:    1
   - Banned IP list:   127.12.12.12
```

Patator (attaque par brutes forces)

Maintenant nous allons tester notre serveur avec des attaques par brutes forces grâce 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.

```
vchantraine@ubuntu:~$ patator ssh login host=192.168.60.128 user=FILE0 0=/home/vchantraine/Documents/user.txt password=FILE1 1=/home/vchantraine/Documents/pass.txt
03:14:05 patator INFO - Starting Patator v0.7 (https://github.com/langette/patator) at 2023-12-11 03:14:05
03:14:05 patator INFO -
03:14:05 patator INFO - code size time candidate num msg
03:14:05 patator INFO - 0 39 0.061 | vchantraine:123456 | 1 | SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.9
03:14:09 patator INFO - 1 22 3.738 | vchantraine:12345 | 2 | Authentication failed.
03:14:09 patator INFO - 1 22 3.744 | vchantraine:123456789 | 3 | Authentication failed.
03:14:09 patator INFO - 1 22 3.739 | vchantraine:nicole | 10 | Authentication failed.
03:14:09 patator INFO - 1 22 3.743 | vchantraine:daniel | 11 | Authentication failed.
03:14:09 patator INFO - 1 22 3.696 | vchantraine:password | 4 | Authentication failed.
03:14:09 patator INFO - 1 22 3.743 | vchantraine:loveyou | 5 | Authentication failed.
03:14:09 patator INFO - 1 22 3.736 | vchantraine:princess | 6 | Authentication failed.
03:14:09 patator INFO - 1 22 3.744 | vchantraine:1234567 | 7 | Authentication failed.
03:14:09 patator INFO - 1 22 3.741 | vchantraine:12345678 | 8 | Authentication failed.
03:14:09 patator INFO - 1 22 3.741 | vchantraine:abc123 | 9 | Authentication failed.
03:14:39 patator INFO - 1 23 30.076 | vchantraine:babygirl | 12 | Authentication timeout.
03:14:39 patator INFO - 1 23 30.088 | vchantraine:monkey | 13 | Authentication timeout.
03:14:39 patator INFO - 1 23 30.075 | vchantraine:lovely | 14 | Authentication timeout.
03:14:39 patator INFO - 1 23 30.068 | vchantraine:654321 | 16 | Authentication timeout.
03:14:39 patator INFO - 1 23 30.083 | vchantraine:111111 | 20 | Authentication timeout.
03:14:39 patator INFO - 1 23 30.088 | vchantraine:iloveu | 21 | Authentication timeout.
03:14:39 patator INFO - 1 23 30.091 | vchantraine:jessica | 15 | Authentication timeout.
03:14:39 patator INFO - 1 23 30.087 | vchantraine:michael | 17 | Authentication timeout.
03:14:39 patator INFO - 1 23 30.078 | vchantraine:ashley | 18 | Authentication timeout.
03:14:39 patator INFO - 1 23 30.093 | vchantraine:qwerty | 19 | Authentication timeout.
03:15:09 patator INFO - 1 23 30.041 | vchantraine:000000 | 22 | Authentication timeout.
03:15:09 patator INFO - 1 23 30.034 | vchantraine:michelle | 23 | Authentication timeout.
03:15:09 patator INFO - 1 23 30.033 | vchantraine:tigger | 24 | Authentication timeout.
03:15:09 patator INFO - 1 23 30.057 | vchantraine:chocolate | 26 | Authentication timeout.
03:15:09 patator INFO - 1 23 30.017 | vchantraine:soccer | 28 | Authentication timeout.
03:15:09 patator INFO - 1 23 30.034 | vchantraine:friends | 30 | Authentication timeout.
03:15:09 patator INFO - 1 23 30.036 | vchantraine:butterfly | 31 | Authentication timeout.
03:15:09 patator INFO - 1 23 30.030 | vchantraine:sunshine | 25 | Authentication timeout.
03:15:09 patator INFO - 1 23 30.033 | vchantraine:password1 | 27 | Authentication timeout.
03:15:09 patator INFO - 1 23 30.030 | vchantraine:anthony | 29 | Authentication timeout.

vchantraine@ubuntu:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
f2b-sshd tcp -- anywhere anywhere multiport dports ssh

Chain FORWARD (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination

Chain f2b-sshd (1 references)
target prot opt source destination
REJECT all -- 192.168.60.132 anywhere reject-with icmp-port-unreachable
REJECT all -- ubuntu anywhere reject-with icmp-port-unreachable
RETURN all -- anywhere anywhere

vchantraine@ubuntu:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed: 10
| '- File list: /var/log/auth.log
'- Actions
| |- Currently banned: 2
| |- Total banned: 2
'- Banned IP list: 192.168.60.128 192.168.60.132
```

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