

## Documentation Installation et Configuration de Fail2ban et Patator avec VirtualBox

### Objectif du Projet

L'objectif de ce projet est d'installer et configurer un filtre de prévention d'intrusion, Fail2ban, sur un système utilisant VirtualBox. Ce filtre vise à contrer les attaques répétées et les attaques par force brute provenant d'une même machine, en particulier les attaques lancées par des robots.

### Installation de Fail2ban

1. Mettre à jour la base de données de paquets :  
```bash  
sudo apt-get update  
```
2. Installer Fail2ban :  
```bash  
sudo apt install fail2ban  
```
3. Démarrer le service Fail2ban :  
```bash  
systemctl start fail2ban  
```
4. Activer le démarrage automatique de Fail2ban :  
```bash  
systemctl enable fail2ban  
```
5. Vérifier l'état de l'installation :  
```bash  
systemctl status fail2ban  
```

### Configuration de Fail2ban

1. Éditer le fichier de configuration personnalisé :  
```bash  
sudo vi /etc/fail2ban/jail.d/custom.conf  
```
2. Ajouter les paramètres de configuration :  
```ini  
[DEFAULT]  
ignoreip = 127.0.0.1  
findtime = 10m  
bantime = 24h  
maxretry = 3  
  
[sshd]  
enabled = true  
port = 22  
logpath = /var/log/auth.log  
maxretry = 5  
```
3. Éditer le fichier principal de configuration :  
```bash  
sudo vi /etc/fail2ban/jail.conf  
```
4. Spécifier les services à surveiller (ex. SSH) :

```

""ini
[sshd]
port = ssh
logpath = %(sshd_log)s
backend = %(sshd_backend)s
""

```

5. Relancer le service Fail2ban :
 

```

""bash
sudo systemctl restart fail2ban
""

```
6. Vérifier les "prisons" actives :
 

```

""bash
sudo fail2ban-client status
""

```

## Déroulement d'une Attaque par Force Brute

1. Installation de Patator (outil de brute force) :
 

```

""bash
sudo apt install patator
""

```
2. Utilisation de deux wordlists pour tester le filtre SSH (Fail2ban).

Commande :

```

""bash
patator ssh_login host=IP target_user=FILE0 password=FILE1 0=users.txt 1=rockyou.txt
""

```

```

virtual2@VM2: ~/Desktop$ cd ..
virtual2@VM2: ~$ hostname -I
192.168.56.102
virtual2@VM2: ~$ patator ssh_login host=192.168.56.101 user=javed password=FILE0 0=/home/virtual2/Desktop/mdp.txt
12:35:14 patator INFO - Starting Patator v0.7 (https://github.com/lanjelot/patator) at 2023-12-11 12:35 CET
12:35:14 patator INFO -
12:35:14 patator INFO - code size time | candidate | num | msg
12:35:14 patator INFO - 0 39 0.059 | 123456 | 1 | SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.9
12:35:18 patator INFO - 1 22 4.172 | 12345 | 2 | Authentication failed.
12:35:18 patator INFO - 1 22 4.172 | 123456789 | 3 | Authentication failed.
12:35:18 patator INFO - 1 22 4.175 | password | 4 | Authentication failed.
12:35:18 patator INFO - 1 22 4.175 | iloveyou | 5 | Authentication failed.
12:35:18 patator INFO - 1 22 4.169 | princess | 6 | Authentication failed.
12:35:18 patator INFO - 1 22 4.165 | 1234567 | 7 | Authentication failed.
12:35:18 patator INFO - 1 22 4.178 | 12345678 | 8 | Authentication failed.
12:35:18 patator INFO - 1 22 4.195 | abc123 | 9 | Authentication failed.
12:35:18 patator INFO - 1 22 4.163 | nicole | 10 | Authentication failed.
12:35:19 patator INFO - 1 22 4.169 | daniel | 11 | Authentication failed.
12:35:20 patator INFO - 1 22 2.067 | babygirl | 12 | Authentication failed.
12:35:20 patator INFO - 1 22 2.066 | lovely | 14 | Authentication failed.
12:35:20 patator INFO - 1 22 2.065 | jennifer | 20 | Authentication failed.
12:35:21 patator INFO - 1 22 2.065 | joshua | 21 | Authentication failed.
12:35:21 patator INFO - 1 22 2.070 | monkey | 13 | Authentication failed.
12:35:21 patator INFO - 1 22 2.067 | 123123 | 15 | Authentication failed.
12:35:21 patator INFO - 1 22 2.065 | football | 16 | Authentication failed.
12:35:21 patator INFO - 1 22 2.069 | secret | 17 | Authentication failed.
12:35:21 patator INFO - 1 22 2.065 | andrea | 18 | Authentication failed.
12:35:21 patator INFO - 1 22 2.068 | carlos | 19 | Authentication failed.
12:35:22 patator INFO - 1 22 2.066 | bubbles | 22 | Authentication failed.
12:35:23 patator INFO - Hits/Done/Skip/Fail/Size: 22/22/0/0/22, Avg: 2 r/s, Time: 0h 0m 8s
virtual2@VM2: ~$

```

3. Fail2ban détecte l'attaque et bloque l'adresse IP de la machine attaquante.

## Vérification des Adresses IP Bloquées

- Avec iptables :

```

""bash
sudo iptables -L
""

```

- Avec Fail2ban :

```

""bash
sudo fail2ban-client status ssh

```

```
jawed@VM1: ~  
Command 'hostname-' not found, did you mean:  
  command 'hostname' from deb hostname (3.23)  
Try: apt install <deb name>  
  
jawed@VM1:~$ hostname -I  
192.168.56.101  
jawed@VM1:~$ sudo fail2ban-client status  
[sudo] password for jawed:  
Status  
|- Number of jail:      1  
|- Jail list:   sshd  
jawed@VM1:~$ sudo fail2ban-client status sshd  
Status for the jail: sshd  
|- Filter  
|- Currently failed: 1  
|- Total failed:    21  
|- File list:       /var/log/auth.log  
|- Actions  
|- Currently banned: 1  
|- Total banned:    1  
|- Banned IP list:  192.168.56.102  
jawed@VM1:~$
```

...

### Conclusion:

Cette documentation présente les étapes d'installation, configuration et utilisation de Fail2ban sur un système VirtualBox, avec un exemple d'attaque par force brute pour illustrer son efficacité.