HAMED Jawed

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
```

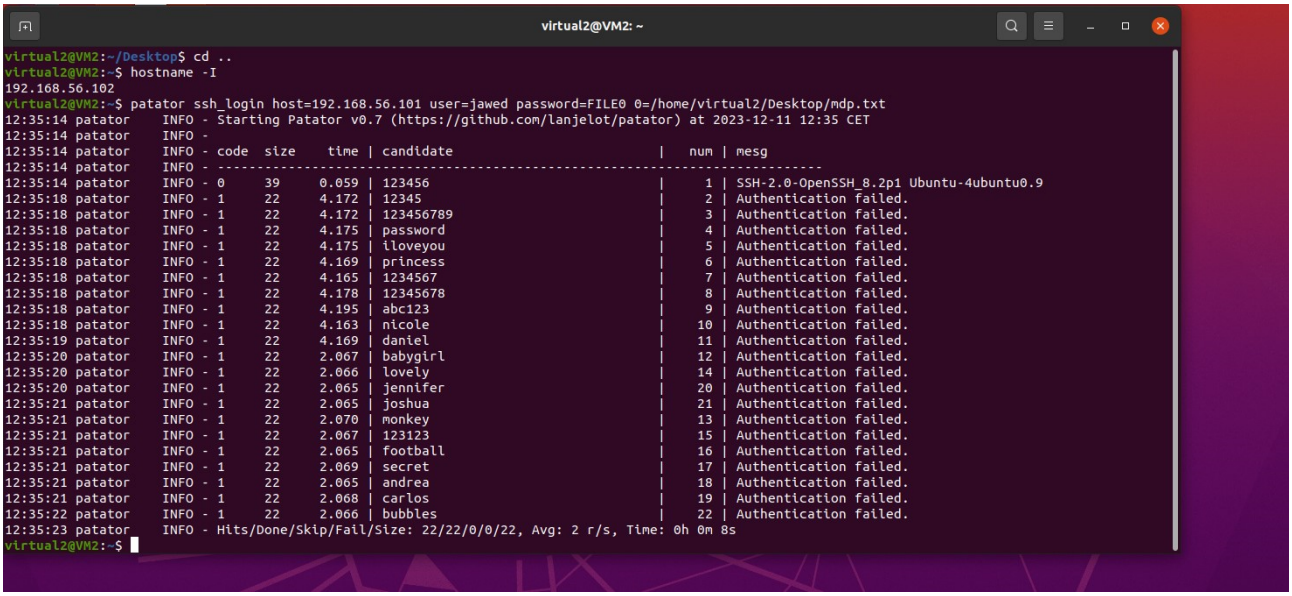
6. Vérifier les "prisons" actives :
```bash
sudo fail2ban-client status
```

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
```

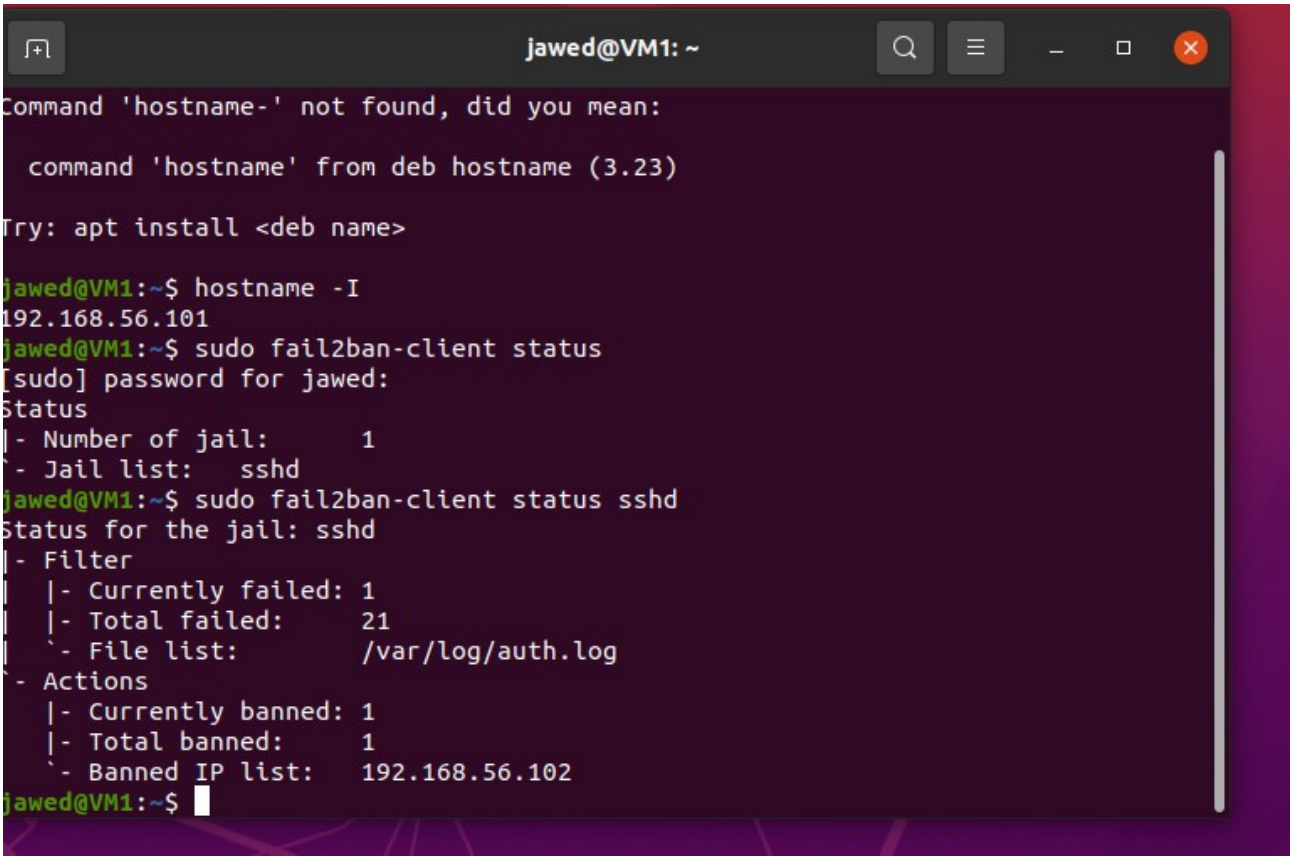


3. Fail2ban détecte l'attaque et bloque l'adresse IP de la machine attaquante.

Vérification des Adresses IP Bloquées

- Avec iptables :
```bash
sudo iptables -L
```

- Avec Fail2ban :
```bash
sudo fail2ban-client status ssh
```




```

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.
```