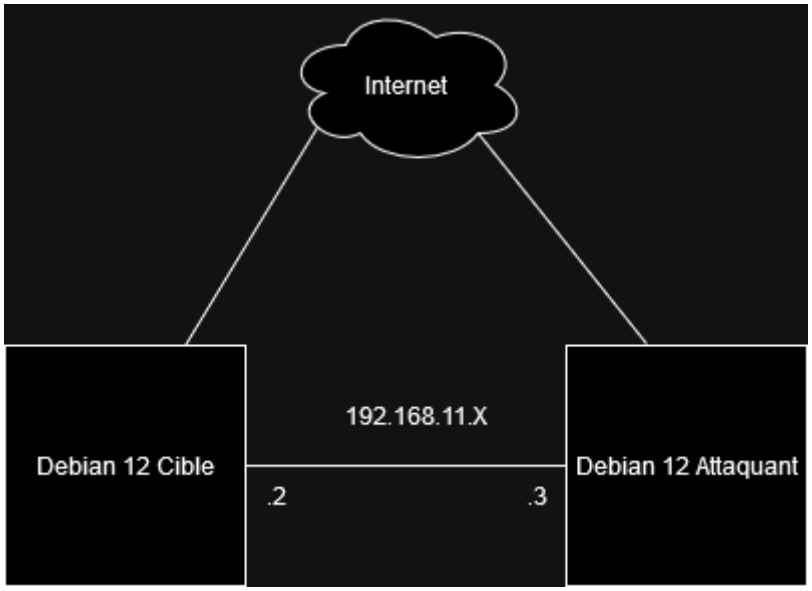
Compte rendu fail2ban

By Valentin LESNES



Attaque par dictionnaire :

Commande depuis l'attaquant :

```
sudo apt install nmap hydra fail2ban -y
```

```
sudo nmap -sS -p- 192.168.11.2
```

```
test@debian:/$ sudo nmap -sS -p- 192.168.11.2
Starting Nmap 7.93 ( https://nmap.org ) at 2024-12-04 09:36 CET
Nmap scan report for 192.168.11.2
Host is up (0.00064s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:0C:29:5E:12:15 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.86 seconds
```

Il y a donc le port ssh (22) d'ouvert.

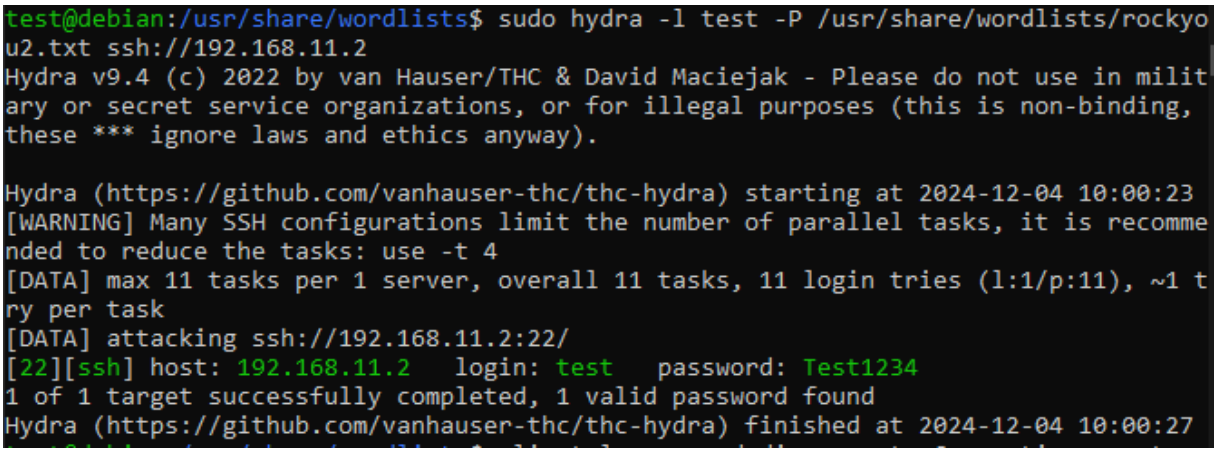
On télécharge le fichier rockyou.txt (https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt&ved=2ahUKEwiptauR5o2KAxUYBfsDHXQ7MG4QFnoECAwQAQ&usg=AOvVaw3snAERl1mU6Ccr4WFEazBd) puis on le met dans le dossier /usr/share/wordlists/ .

On lance l'attaque avec cette commande :

sudo hydra -l test -P /usr/share/wordlists/rockyou.txt ssh://192.168.11

Le fichier rockyou.txt étant beaucoup trop gros pour notre test créé le rockyou2.txt avec des mots de passe aléatoire et on met bien sur le vrai mot de passe.

Si cela à bien fonctionner on doit avoir cela :



On a bien récupéré le mot de passe.

<u>Défense avec fail2ban :</u>

Sur la machine cible :

On installe rsyslog :

```
sudo apt install -y fail2ban iptables rsyslog
```

Puis on modifie le fichier jail.conf en jail.local :

```
sudo cp /etc/fail2ban/jail.{conf,local}
```

On créé le fichier auth.log :

```
sudo touch /var/log/auth.log
```

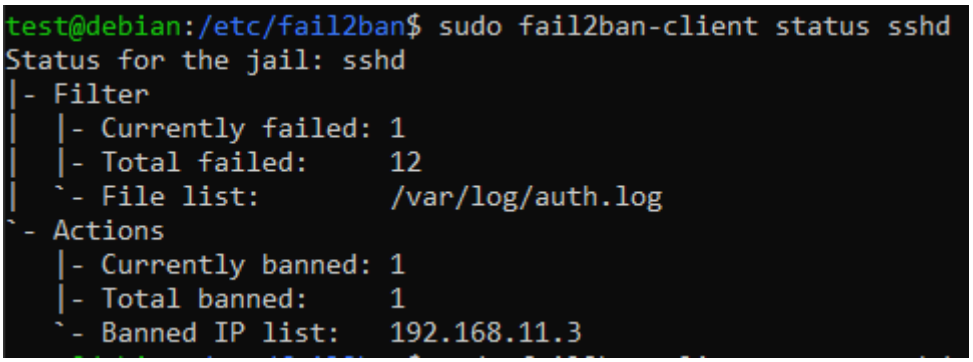
Puis on restart le service fail2ban :

```
sudo systemctl restart fail2ban
```

On réessaye l'attaque et normalement l'attaquant doit être bloquer.

Pour voir les logs :

```
sudo fail2ban-client status
sudo fail2ban-client status sshd
```


test@debian:/etc/fail2ban$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 1
| |- Total failed: 12
| `- File list: /var/log/auth.log
`- Actions
   |- Currently banned: 1
   |- Total banned: 1
   `- Banned IP list: 192.168.11.3