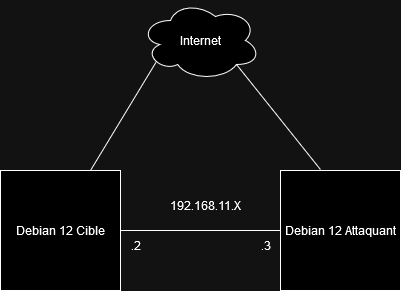
**Compte rendu fail2ban**

By Valentin LESNES

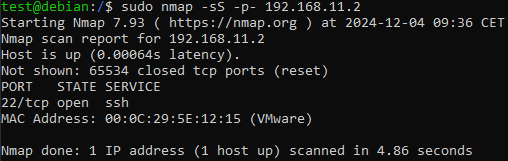


Attaque par dictionnaire :

Commande depuis l’attaquant :

sudo apt install nmap hydra fail2ban -y

sudo nmap -sS -p- 192.168.11.2



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

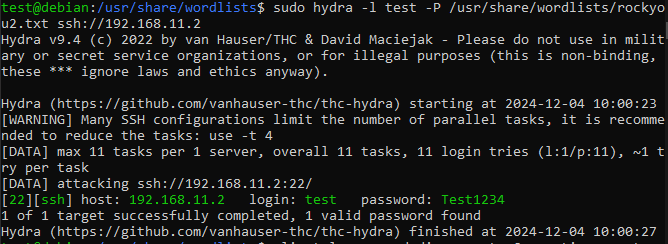
On télécharge le fichier rockyou.txt (<https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt&ved=2ahUKEwiptauR5o2KAxUYBfsDHXQ7MG4QFnoECAwQAQ&usg=AOvVaw3snAERl1mU6Ccr4WFEazBd>) puis on le met dans le dossier /usr/share/wordlists/ .

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.

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 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

