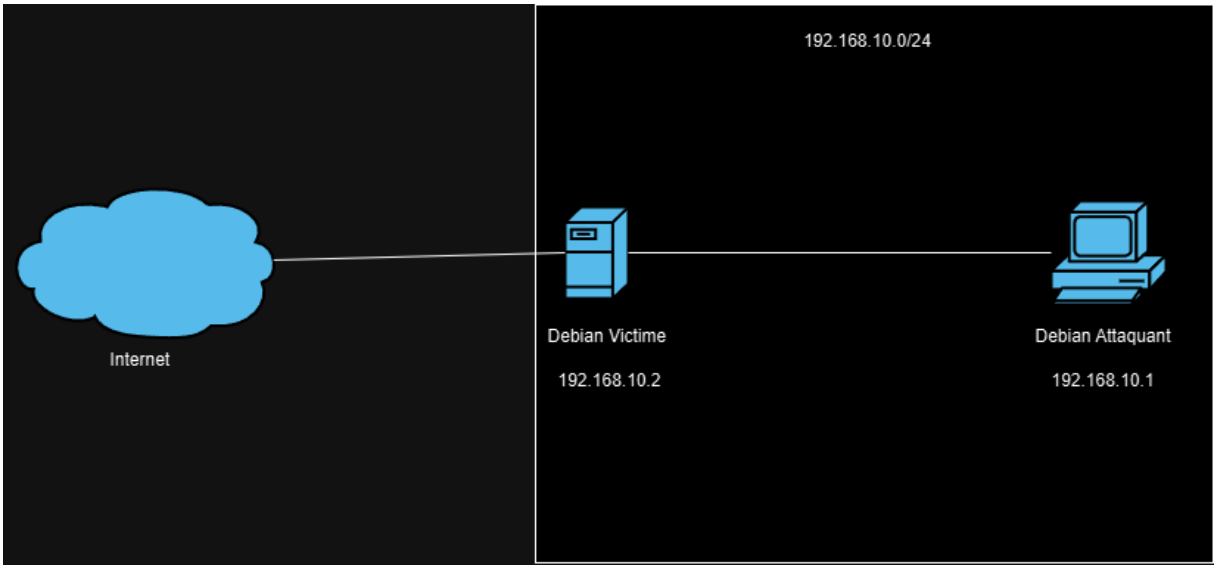
TP8 Fail2Ban

By Teo PANEI

Schéma Réseau :



Prérequis : Installez deux machines virtuelles Ubuntu (ou une autre distribution Linux).

Pour ma part j'ai utilisé 2 machine sous Debian 12

Première étape : Installez Nmap Hydra et fail2ban sur la machine de l'attaquant et la cible.

sudo apt install nmap hydra fail2ban -y

```
teoop@debianattaquant:~$ sudo apt install nmap hydra fail2ban
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
nmap est déjà la version la plus récente (7.93+dfsg1-1).
hydra est déjà la version la plus récente (9.4-1).
fail2ban est déjà la version la plus récente (1.0.2-2).
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
```

Deuxième étape : Scan de ports (ATTAQUE)

Sur la machine d'attaque, exécutez la commande suivante pour scanner les ports de la cible

nmap -sS -p- [IP_de_la_cible]

```
teoop@debianattaquant:~$ sudo nmap -sS -p- 192.168.10.2
[sudo] Mot de passe de teoop :
Starting Nmap 7.93 ( https://nmap.org ) at 2024-12-04 09:50 CET
Nmap scan report for 192.168.10.2
Host is up (0.00062s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:0C:29:6C:54:E1 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.19 seconds
```

On peut constater que le port 22 est ouvert pour le service SSH.

Troisième étape : Force Brute

Sur la machine attaquante, utilisez hydra pour lancer une attaque par force brute sur le compte

Commande de base :

Sudo hydra -l test -P /usr/share/wordlists/rockyou.txt ssh://[IP_de_la_cible]

Celle que j'ai fait :

Sudo hydra -l test -P /usr/share/wordlists/Rockyou1.txt ssh://[IP_de_la_cible]

```
teoop@debianattaquant:~$ sudo hydra -l teoop -P /usr/share/wordlists/Rockyou1.txt ssh://192.168.10.2
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret servi
ce organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anywa
y).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-04 10:34:25
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the
tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 18 login tries (l:1/p:18), ~2 tries per task
[DATA] attacking ssh://192.168.10.2:22/
[22][ssh] host: 192.168.10.2   login: teoop   password: fidjy@1710
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-04 10:34:29
```

Pour moi j'ai créé un document en inventant des mots de passe et parmi cette liste j'ai mis mon mot de passe que j'ai nommé Rockyou1.txt

Quatrième étape : Défense avec Fail2ban

Fail2ban est un outil qui analyse les journaux du système et bannit les IPs qui présentent un comportement suspect (par exemple, trop d'échecs de connexion).

Configuration de fail2ban :

Sudo apt-get install rsyslog

sudo nano /etc/fail2ban/jail.local

sudo apt install -y fail2ban iptables

sudo mv /etc/fail2ba,/jail.conf /etc/fail2ban/fail.local

Redémarrez Fail2ban pour appliquer les modifications :

Sudo systemctl status fail2ban.service

Testez la configuration :

Sur la machine d'attaque, refaites l'attaque par force brute avec `hydra`.

Après quelques tentatives d'échec, l'IP de l'attaquant devrait être bannie par Fail2ban.

```
teoop@debianattaquant:/usr/share/wordlists$ sudo hydra -l teoop -P /usr/share/wordlists/Rockyou1.txt s
sh://192.168.10.2
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret servi
ce organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anywa
y).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-04 11:33:09
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the
tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previou
s session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 18 login tries (l:1/p:18), ~2 tries per task
[DATA] attacking ssh://192.168.10.2:22/
[ERROR] could not connect to ssh://192.168.10.2:22 - Connection refused
```

On remarque que depuis l'attaquant on ne plus se connecter en ssh a la cible ce qui veut dire que le Fail2ban est bien opérationnel et sert à filtrer

Analyse des journaux :

Sudo mkdir /var/log/auth.log (si il est pas déjà créer)

sudo fail2ban-client status sshd

```
teoop@debianvictime:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 1
|  |- Total failed:     39
|  `- File list:        /var/log/auth.log
`- Actions
   |- Currently banned: 1
   |- Total banned:     3
   `- Banned IP list:   192.168.10.1
```

On remarque que le fail2ban a bien banni l'IP de l'attaquant :

En conclusion : Ce TP nous permet de savoir comment marche une attaque par dictionnaire mais aussi à comment nous protéger de cette attaque avec Fail2ban