

Notice SAÉ 1.1 2024 HYDRA

Dans un premier lieu on va installer une VM et sur cette dernière, la paramétrer afin de pouvoir utiliser hydra en ssh sur cette machine virtuelle :

Pour ce faire on prend une image de VM, on l'insère dans le logiciel Virtual BOX ou VMware (on utilisera VBOX) et une fois ça fais, on la lance.

On installe et on la paramètre pour la connexion SSH :

```
apt install openssh-server
```

```
systemctl status ssh
```

```
root@debian-10:/etc# apt install openssh-server
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
openssh-server est déjà la version la plus récente (1:7.9p1-10+deb10u2).
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
root@debian-10:/etc#
```

```
root@debian-10:/etc# apt install openssh-server
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
openssh-server est déjà la version la plus récente (1:7.9p1-10+deb10u2).
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
root@debian-10:/etc# systemctl status ssh
• ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2024-10-22 08:30:34 CEST; 1h 2min ago
     Docs: man:sshd(8)
           man:sshd_config(5)
  Main PID: 14813 (sshd)
    Tasks: 1 (limit: 2359)
   Memory: 1.5M
   CGroup: /system.slice/ssh.service
           └─14813 /usr/sbin/sshd -D

oct. 22 09:12:50 debian-10 sshd[14933]: Failed password for invalid user admin from 172.21.1.54 port
oct. 22 09:12:52 debian-10 sshd[14933]: Connection closed by invalid user admin 172.21.1.54 port 463
oct. 22 09:13:31 debian-10 sshd[14935]: Invalid user admin from 172.21.1.54 port 53614
oct. 22 09:13:31 debian-10 sshd[14935]: Received disconnect from 172.21.1.54 port 53614:11: Bye Bye
oct. 22 09:13:31 debian-10 sshd[14935]: Disconnected from invalid user admin 172.21.1.54 port 53614
oct. 22 09:13:32 debian-10 sshd[14937]: Invalid user admin from 172.21.1.54 port 53624
oct. 22 09:13:32 debian-10 sshd[14937]: pam_unix(sshd:auth): check pass; user unknown
oct. 22 09:13:32 debian-10 sshd[14937]: pam_unix(sshd:auth): authentication failure; logname= uid=0
oct. 22 09:13:34 debian-10 sshd[14937]: Failed password for invalid user admin from 172.21.1.54 port
oct. 22 09:13:36 debian-10 sshd[14937]: Connection closed by invalid user admin 172.21.1.54 port 536
lines 1-21/21 (END)
```

On récupère ensuite l'adresse IP de la machine virtuel :

```
ip a
```

```
root@debian-10:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:51:84:fe brd ff:ff:ff:ff:ff:ff
    inet 172.21.212.92/16 brd 172.21.255.255 scope global dynamic enp0s3
        valid_lft 2752sec preferred_lft 2752sec
    inet6 fe80::a00:27ff:fe51:84fe/64 scope link
        valid_lft forever preferred_lft forever
root@debian-10:~# _
```

On note l'adresse IP de notre VM qui nous sera utile avec Hydra.

Par la suite sur notre machine principale on installer Hydra et initialiser le bruteforce par connexion SSH :

```
apt install hydra
```

```
adminetu@LinuxDebianGUI:~$ sudo apt install hydra
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
hydra est déjà la version la plus récente (9.4-1).
0 mis à jour, 0 nouvellement installés, 0 à enlever et 88 non mis à jour.
adminetu@LinuxDebianGUI:~$
```

Après ça on télécharge un dictionnaire ou on en créer un, pour ma part j'ai créer un dictionnaire avec le mot de passe de la machine virtuel pour vérifier que cela marche directement.

```
hydra -l root -P /home/adminetu/Bureau/psw.txt 172.21.212.92
```

L'option -l signifie login, donc le login de la session (root sur la VM), l'option -P est pour l'utilisation d'un dictionnaire (nous c'est psw.txt), puis l'adresse IP de la target et le type de connexion (SSH).

```
adminetu@LinuxDebianGUI:~$ hydra -l root -P /home/adminetu/Bureau/psw.txt 172.21.212.92 ssh
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 2024-10-22 10:06:10
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:l/p:1), ~1 try per task
[DATA] attacking ssh://172.21.212.92:22/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-22 10:06:14
adminetu@LinuxDebianGUI:~$
```

Initialement on devrait trouvé le mdp car à l'intérieur du dictionnaire on a Root1 qui est le mdp de la VM.