

LRB – SIO1 - SSH Secure Shell

1) Installation de serveur SSH sur Vm Linux

-J'ai installé le serveur SSH grâce à la commande : `sudo apt install openssh-server`.

-Puis j'ai générer les clés ssh afin de s'authentifier entre hôte sans mot de passe grâce à la commande suivante : `ssh-keygen -t rsa`.

-Puis j'ai copié le fichier `home/anish/.ssh/id_rsa.pub` ou la clé privée est enregistré par défaut et l'ajouté à `home/anish/.ssh/authorised_keys` grâce à la commande suivante : `ssh-copy id anish@ubuntu`.

-Maintenant je vais pouvoir me connecter à mon serveur ssh sans mot de passe en tapant : SSH anish@ubuntu.

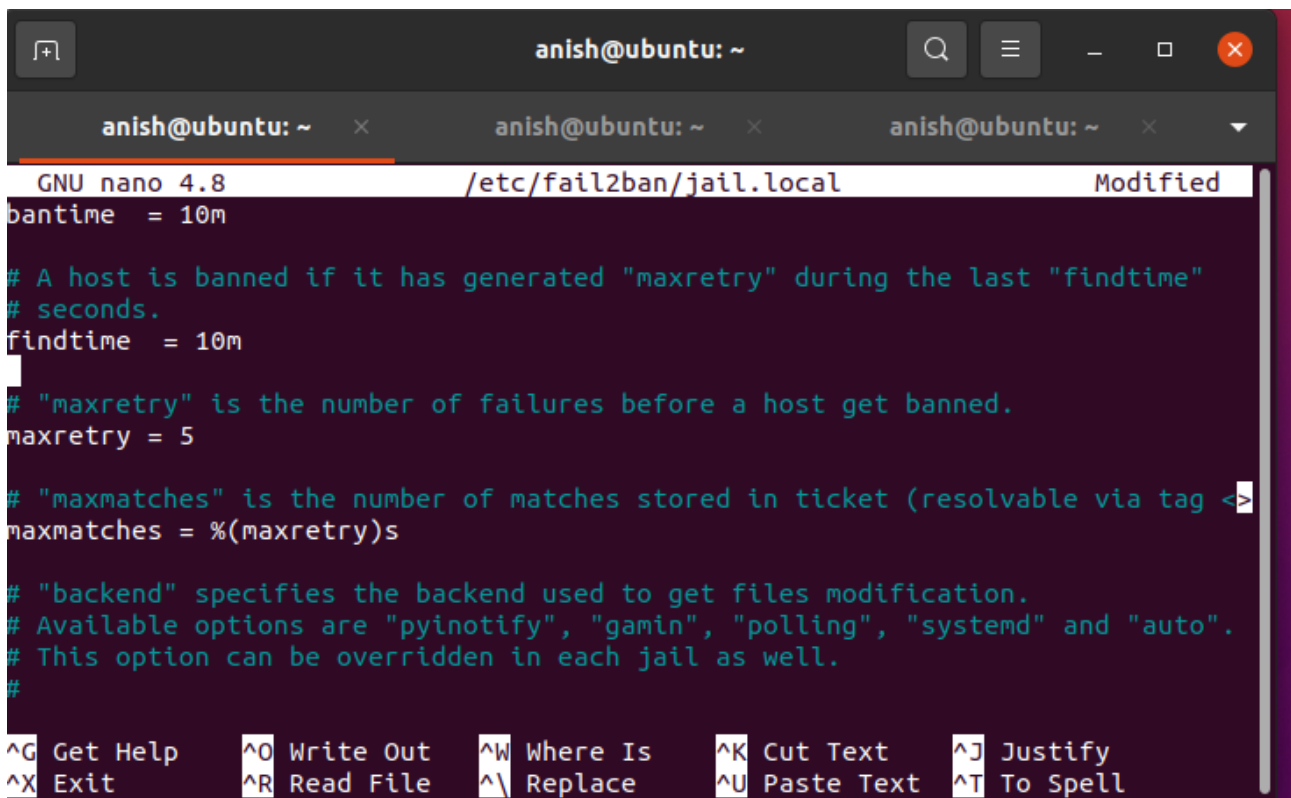
Nano `etc/ssh/sshd_config` : permet de configurer le serveur SSH.

2) Installation de fail2ban

-Pour sécuriser mon serveur ssh j'ai installé fail2ban. `Sudo apt install fail2ban`.

-Ensuite pour configurer le serveur fail2ban j'ai d'abord copié le fichier `etc/fail2ban/jail.conf` en `jail.local` au cas ou le fichier `jail.conf` serait dédommager.

-Puis grâce à la commande : `sudo nano etcfail2ban/jail.local` j'ai ouvert le fichier et je pouvais regarder et modifier le contenu du fichier par exemple je peux modifier le temps de bannissement, puis j'ai ban mon propre ip (127,0,0,1) et vérifié si je pouvais me connecter au serveur ssh et je ne pouvais plus m'accéder à mon serveur SSH. J'ai aussi essayé de me connecter depuis Windows grâce à l'invité de commandes.



```
anish@ubuntu: ~
GNU nano 4.8 /etc/fail2ban/jail.local Modified
bantime = 10m

# A host is banned if it has generated "maxretry" during the last "findtime"
# seconds.
findtime = 10m

# "maxretry" is the number of failures before a host get banned.
maxretry = 5

# "maxmatches" is the number of matches stored in ticket (resolvable via tag <>
maxmatches = %(maxretry)s

# "backend" specifies the backend used to get files modification.
# Available options are "pyinotify", "gamin", "polling", "systemd" and "auto".
# This option can be overridden in each jail as well.
#

^G Get Help      ^O Write Out    ^W Where Is     ^K Cut Text     ^J Justify
^X Exit          ^R Read File    ^\ Replace      ^U Paste Text   ^T To Spell
```

```
anish@ubuntu: ~  
Microsoft Windows [version 10.0.19043.1526]  
(c) Microsoft Corporation. Tous droits réservés.  
  
C:\Users\cdfak>ssh anish@192.168.118.129  
anish@192.168.118.129's password:  
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.13.0-28-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:       https://ubuntu.com/advantage  
  
122 updates can be applied immediately.  
33 of these updates are standard security updates.  
To see these additional updates run: apt list --upgradable  
  
Your Hardware Enablement Stack (HWE) is supported until April 2025.  
Last login: Thu Mar 10 02:39:41 2022 from 127.0.0.1  
anish@ubuntu:~$
```

J'ai réussi à me connecter depuis l'invité de commandes.

```
Connection to 192.168.118.129 closed.  
  
C:\Users\cdfak>ssh anish@192.168.118.129  
anish@192.168.118.129's password:  
Permission denied, please try again.  
anish@192.168.118.129's password:  
Permission denied, please try again.  
anish@192.168.118.129's password:  
anish@192.168.118.129: Permission denied (publickey,password).  
  
C:\Users\cdfak>
```

Je me suis déconnecter et j'ai essayé de me connecter et mettant un faux mot de passe et on remarque qu'au bout de 3 tentatives je n'avais plus le permission de me connecter (j'ai mis maxretry 3 dans le fichier jail.local).

```
anish@ubuntu:~$ sudo fail2ban-client status sshd  
[sudo] password for anish:  
Status for the jail: sshd  
|- Filter  
| |- Currently failed: 1  
| |- Total failed: 1  
| `-- File list: /var/log/auth.log  
`- Actions  
    |- Currently banned: 0  
    |- Total banned: 0  
    `-- Banned IP list:  
anish@ubuntu:~$
```

Puis j'ai vérifier sur fail2ban grâce et on remarque dans currently failed il y a eu 1 ce qui veut dire qu'il y a eu une tentative de connexion qui a échoué.

```
anish@ubuntu: ~  
anish@ubuntu:~$ sudo fail2ban-client set sshd banip 127.0.0.1  
1  
anish@ubuntu:~$ sudo fail2ban-client set sshd unbanip 127.0.0.1  
1  
anish@ubuntu:~$ sudo fail2ban-client set sshd banip 127.0.0.1  
1  
anish@ubuntu:~$ sudo fail2ban-client set sshd unbanip 127.0.0.1  
1  
anish@ubuntu:~$ sudo fail2ban-client status sshd  
[sudo] password for anish:  
Status for the jail: sshd  
|- Filter  
| |- Currently failed: 0  
| |- Total failed: 0  
| `-- File list: /var/log/auth.log  
`-- Actions  
    |- Currently banned: 0  
    |- Total banned: 2  
    `-- Banned IP list:  
anish@ubuntu:~$
```

En tapant la commande `sudo fail2ban-client status sshd` je peux voir l'état de fail2ban, s'il y a eu des tentatives de connexion ratés ou encore les adresse ip banni. J'ai aussi ban mon propre adresse ip manuellement puis j'ai dé banni et on peut remarquer que dans total banned il y a 1 adresse IP banni.

```
anish@ubuntu: ~  
anish@ubuntu:~$ ssh anish@ubuntu  
ssh: connect to host ubuntu port 22: Connection refused  
anish@ubuntu:~$ ssh anish@ubuntu  
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.13.0-28-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
122 updates can be applied immediately.  
83 of these updates are standard security updates.  
To see these additional updates run: apt list --upgradable  
  
Your Hardware Enablement Stack (HWE) is supported until April 2025.  
Last login: Sat Feb 19 07:27:33 2022 from 127.0.0.1  
anish@ubuntu:~$
```

On peut remarquer que ma connexion a été refusé et après avoir dé banni je pouvais me connecter à nouveau.

3) Connexion automatique au serveur grâce à un programme en python

```
1 import paramiko
2
3 command = "df"
4
5
6 host = "192.168.118.129"
7 port= 22
8 username = "anish@ubuntu"
9 password = "skedk"
10
11 client = paramiko.client.SSHClient()
12 client.set_missing_host_key_policy(paramiko.AutoAddPolicy())
13 client.connect(host, port=port, username=username, password=password)
14 _stdin, stdout, stderr = client.exec_command("df")
15 print(stdout.read().decode())
16 client.close()
```

J'ai taper ce programme qui permet automatiquement de se connecter sur le serveur SSH.
Et j'ai essayé de me connecter avec un faux mot de passe et après 3 tentatives mon adresse IP a été banni.

```
anish@ubuntu:~/Desktop$ python3 ssh_connexion.py
Traceback (most recent call last):
  File "ssh_connexion.py", line 15, in <module>
    client.connect(host, port=port, username=username, password=password)
  File "/usr/lib/python3/dist-packages/paramiko/client.py", line 368, in connect
    raise NoValidConnectionsError(errors)
paramiko.ssh_exception.NoValidConnectionsError: [Errno None] Unable to connect to port 22 on 192.168.118.129
```

```
anish@ubuntu:/$ sudo fail2ban-client status sshd
[sudo] password for anish:
Status for the jail: sshd
|- Filter
| |- Currently failed: 1
| |- Total failed:      8
| `-- File list:        /var/log/auth.log
`- Actions
  |- Currently banned: 1
  |- Total banned:     2
  `-- Banned IP list:   192.168.118.129
anish@ubuntu:/$
```