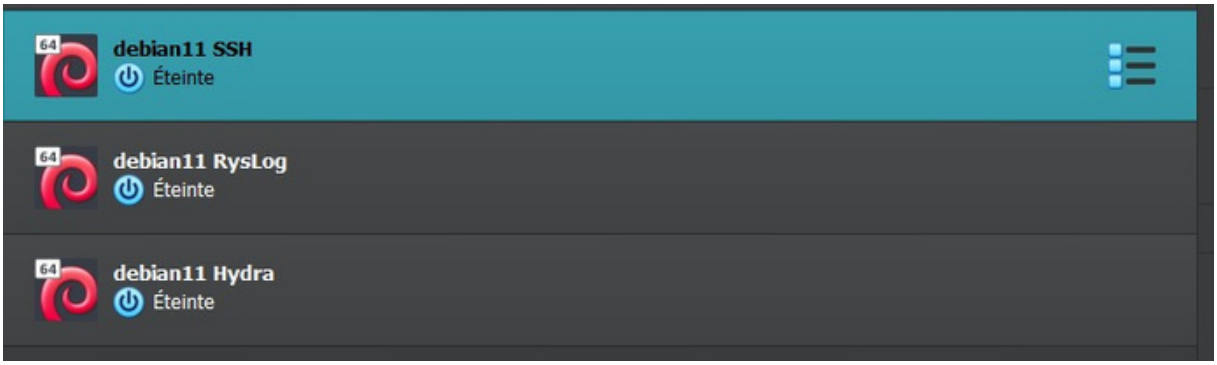
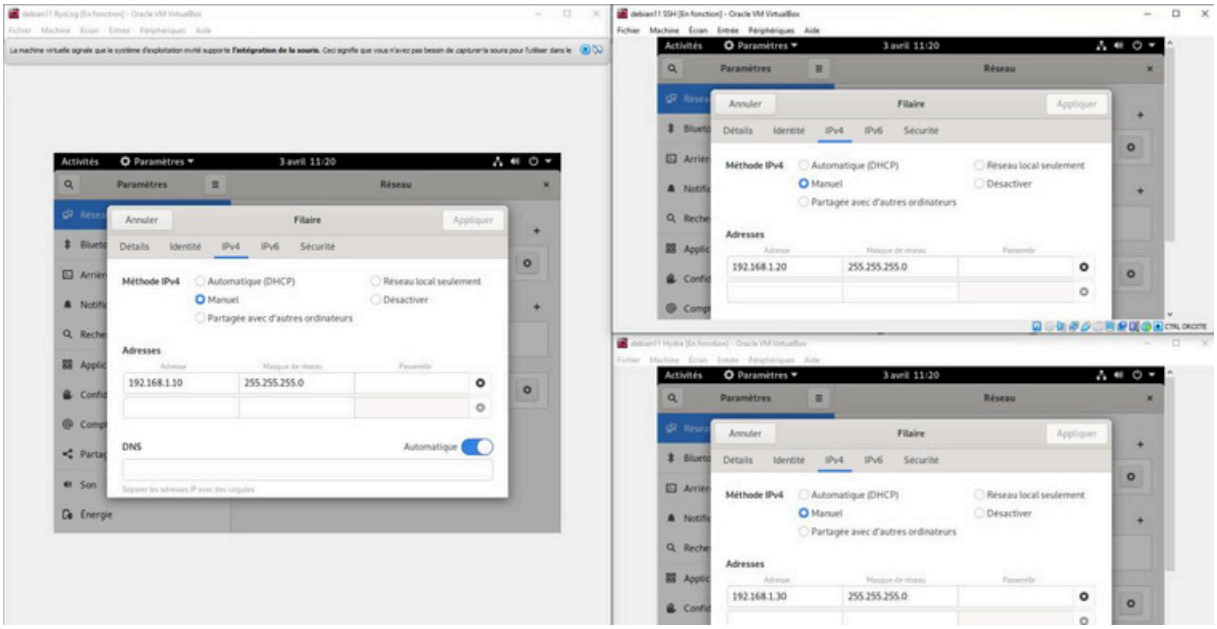
Utilisation de Rsyslog pour la centralisation des logs et la simulation d'une attaque par brute force sur le service SSH.

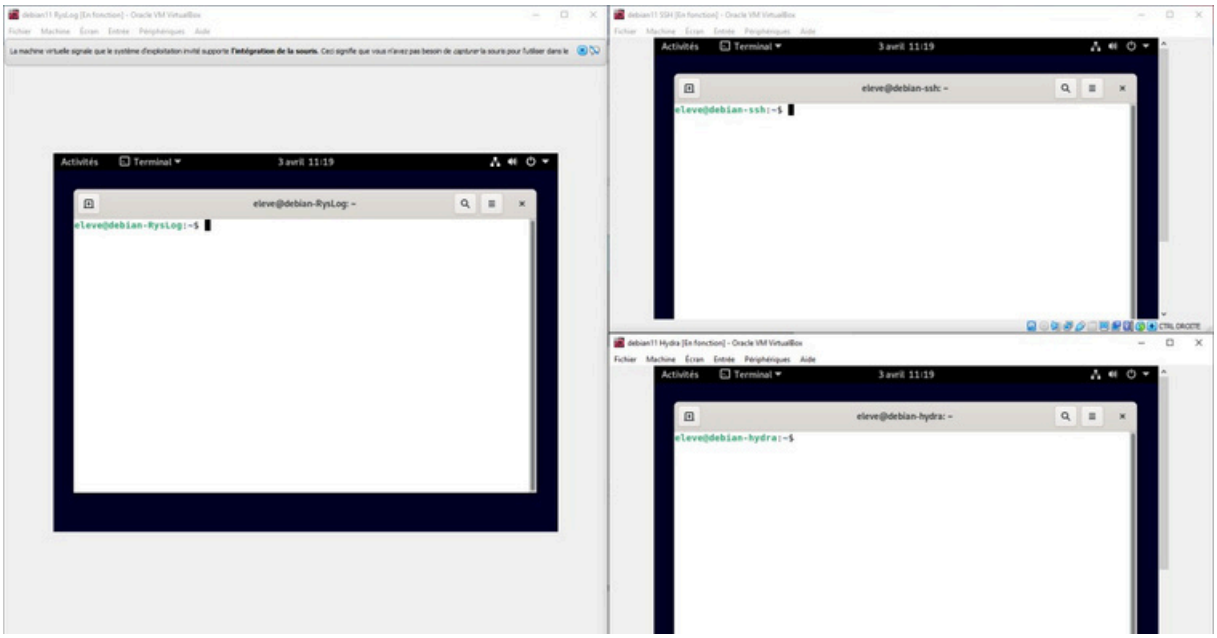
Importation des VM :



Une fois les machines lancer on configure les ip :



Pour renommer les machines on fait cette commande :
sudo hostnamectl set-hostname nomde la machine



Pour la machine hydra on fait apt-get install hydra afin de l'installer et apt-get update pour mettre à jour et ensuite apt-get upgrade

```
root@debian-hydra:~# apt-det install hydra
-bash: apt-det : commande introuvable
root@debian-hydra:~# apt-get 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 (9.1-1).
0 mis à jour, 0 nouvellement installés, 0 à enlever et 1 non mis à jour.

root@debian-hydra:~# apt-get update
Err :1 http://security.debian.org/debian-security bullseye-security InRelease
  Ne parvient pas à résoudre « security.debian.org »
Err :2 http://deb.debian.org/debian bullseye InRelease
  Ne parvient pas à résoudre « deb.debian.org »
Err :3 http://deb.debian.org/debian bullseye-updates InRelease
  Ne parvient pas à résoudre « deb.debian.org »
Lecture des listes de paquets... Fait

root@debian-hydra:~# apt-get upgrade
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Calcul de la mise à jour... Fait
Les paquets suivants ont été conservés :
  linux-image-amd64
0 mis à jour, 0 nouvellement installés, 0 à enlever et 1 non mis à jour.
root@debian-hydra:~#
```

On fait apt-get update et apt-get upgrade pour metre à jour ryslog

```
eleve@debian-RysLog:~$ su -
Mot de passe :
root@debian-RysLog:~# apt-get update
Atteint :1 http://deb.debian.org/debian bullseye InRelease
Atteint :2 http://deb.debian.org/debian bullseye-updates InRelease
Atteint :3 http://security.debian.org/debian-security bullseye-security InReleas
e
Lecture des listes de paquets... Fait
root@debian-RysLog:~# apt-get upgrade
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Calcul de la mise à jour... Fait
Les paquets suivants ont été conservés :
  linux-image-amd64
Les paquets suivants seront mis à jour :
  apache2 apache2-bin apache2-data apache2-doc apache2-utils bind9-dnsutils
  bind9-host bind9-libs firefox-esr firefox-esr-l10n-fr
  gir1.2-javascriptcoregtk-4.0 gir1.2-webkit2-4.0 libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap libcurl3-gnutls libcurl4 libde265-0
  libgnutls30 libjavascriptcoregtk-4.0-18 libnss3 libssl1.1 libtiff5
  libwebkit2gtk-4.0-37 openssl sudo tzdata xserver-common xserver-xephyr
  xserver-xorg-core xserver-xorg-legacy xwayland
```

Pour la machine ssh

On fait apt-get install openssh-server et apt-get update

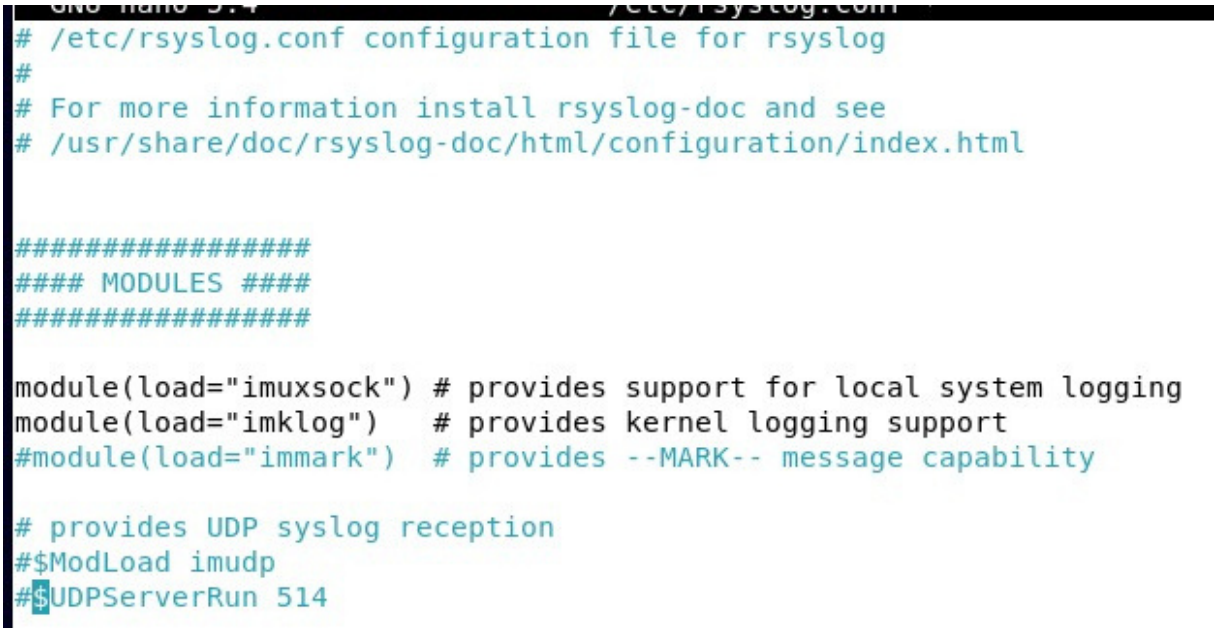
```
E: Impossible de trouver le paquet openssh
root@debian-ssh:~# apt-get install openssh-server
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
openssh-server est déjà la version la plus récente (1:8.4p1-5+deb11u1).
openssh-server passé en « installé manuellement ».
0 mis à jour, 0 nouvellement installés, 0 à enlever et 1 non mis à jour.
root@debian-ssh:~# apt-get install openssh
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
E: Impossible de trouver le paquet openssh
root@debian-ssh:~# apt-get update
Atteint :1 http://security.debian.org/debian-security bullseye-security InRele
e
Atteint :2 http://deb.debian.org/debian bullseye InRelease
Atteint :3 http://deb.debian.org/debian bullseye-updates InRelease
Lecture des listes de paquets... Fait
```

Ensuite apt-get upgrade

```
root@debian-ssh:~# apt-get upgrade
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Calcul de la mise à jour... Fait
Les paquets suivants ont été conservés :
  linux-image-amd64
0 mis à jour, 0 nouvellement installés, 0 à enlever et 1 non mis à jour.
root@debian-ssh:~#
```

```
root@debian-RysLog:~# nano /etc/rsyslog.conf
```

Ensuite : on retire les #, des deux dernières ligne du screen



```
# /etc/rsyslog.conf configuration file for rsyslog
#
# For more information install rsyslog-doc and see
# /usr/share/doc/rsyslog-doc/html/configuration/index.html


#################
#### MODULES ####
#################

module(load="imuxsock") # provides support for local system logging
module(load="imklog")   # provides kernel logging support
#module(load="immark")  # provides --MARK-- message capability

# provides UDP syslog reception
#$ModLoad imudp
#$UDPServerRun 514
```

et on sauvegarde

Ensuite on fait

systemctl restart rsyslog

et

ss- lunlp | grep 514

```
oot@debian-RysLog:~# systemctl restart rsyslog
oot@debian-RysLog:~# ss -tunlp | grep 514
dp   UNCONN 0      0            0.0.0.0:514        0.0.0.0:*    users:(("rsysl
d",pid=4133,fd=6))

dp   UNCONN 0      0               [::]:514           [::]:*    users:(("rsysl
d",pid=4133,fd=7))
```

Toujours sur la vm Ryslog on va installer net-tools avec :

apt-get install net-tools

```
root@debian-RysLog:~# apt-get install net-tools
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les NOUVEAUX paquets suivants seront installés :
  net-tools
0 mis à jour, 1 nouvellement installés, 0 à enlever et 1 non mis à jour.
Il est nécessaire de prendre 250 ko dans les archives.
Après cette opération, 1 015 ko d'espace disque supplémentaires seront utilisé
Réception de :1 http://deb.debian.org/debian bullseye/main amd64 net-tools amd
 1.60+git20181103.0eebece-1 [250 kB]
250 ko réceptionnés en 0s (1 898 ko/s)
Sélection du paquet net-tools précédemment désélectionné.
(Lecture de la base de données... 143819 fichiers et répertoires déjà installé
)
Préparation du dépaquetage de .../net-tools_1.60+git20181103.0eebece-1_amd64.d
 ...
Dépaquetage de net-tools (1.60+git20181103.0eebece-1) ...
Paramétrage de net-tools (1.60+git20181103.0eebece-1) ...
Traitement des actions_différées (« triggers ») pour man-db (2.9.4-2) ...
```

Ensuite :

apt-get update et apt-get upgrade :

```
root@debian-RysLog:~# apt-get update
Atteint :1 http://deb.debian.org/debian bullseye InRelease
Atteint :2 http://security.debian.org/debian-security bullseye-security InReleas
e
Atteint :3 http://deb.debian.org/debian bullseye-updates InRelease
Lecture des listes de paquets... Fait
```

```
root@debian-RysLog:~# apt-get upgrade
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Calcul de la mise à jour... Fait
Les paquets suivants ont été conservés :
  linux-image-amd64
0 mis à jour, 0 nouvellement installés, 0 à enlever et 1 non mis à jour.
root@debian-RysLog:~#
```

et on fait netstat -nul:

```
root@debian-RysLog:~# netstat -nul
Connexions Internet actives (seulement serveurs)
Proto Recv-Q Send-Q Adresse locale          Adresse distante        Etat
udp        0      0 0.0.0.0:38898           0.0.0.0:*
udp        0      0 0.0.0.0:5353            0.0.0.0:*
udp        0      0 0.0.0.0:514             0.0.0.0:*
udp        0      0 0.0.0.0:631             0.0.0.0:*
udp6       0      0 :::37756                :::*
udp6       0      0 :::5353                 :::*
udp6       0      0 :::514                  :::*
```

On voit bien le port 514

Maintenant on va sur la machine ssh

et on exécute cette commande :

```
root@debian-ssh:~# nano /etc/rsyslog.conf

#
# First some standard log files.  Log by facility.
#
auth,authpriv.*                 /var/log/auth.log
*.*;auth,authpriv.none          -/var/log/syslog
#cron.*                         /var/log/cron.log
daemon.*                        -/var/log/daemon.log
kern.*                          -/var/log/kern.log
lpr.*                           -/var/log/lpr.log
mail.*                          -/var/log/mail.log
user.*                          -/var/log/user.log
```

Ici on va ajouter la ligne :

Auth ,authpriv.* @192.168.1.10:514

```
# First some standard log files.  Log by facility.
#
auth,authpriv.*                 /var/log/auth.log
auth,authpriv.*                 @192.168.1.10:514
*.*;auth,authpriv.none          -/var/log/syslog
#cron.*                         /var/log/cron.log
daemon.*                        -/var/log/daemon.log
kern.*                          -/var/log/kern.log
lpr.*                           -/var/log/lpr.log
mail.*                          -/var/log/mail.log
user.*                          -/var/log/user.log
```

On retourne sur rsyslog et on exécute cette commande :

```
root@debian-Ryslog:~# tail -f /var/log/auth.log
Apr  5 20:58:33 debian-Ryslog realmd[924]: stopping service
Apr  5 20:58:35 debian-ssh su: (to root) eleve on pts/0
Apr  5 20:58:35 debian-ssh su: pam_unix(su-l:session): session opened for user
oot(uid=0) by (uid=1000)
Apr  5 20:59:04 debian-Ryslog su: (to root) eleve on pts/0
Apr  5 20:59:04 debian-Ryslog su: pam_unix(su-l:session): session opened for us
r root(uid=0) by (uid=1000)
```

Pour voir les logs d'authentification

Maintenant on peut voir les tentatives de connexion sur la machine ssh

On retourne sur la machine ssh pour effectuer cette commande afin d'ajouter un nouvel utilisateur :

```
oot@debian-ssh:~# adduser johndoe
jout de l'utilisateur « johndoe » ...
jout du nouveau groupe « johndoe » (1001) ...
jout du nouvel utilisateur « johndoe » (1001) avec le groupe « johndoe » ..
réation du répertoire personnel « /home/johndoe »...
opie des fichiers depuis « /etc/skel »...
ouveau mot de passe :
etapez le nouveau mot de passe :
asswd: password updated successfully
hanging the user information for johndoe
nter the new value, or press ENTER for the default
        Full Name []: John
        Room Number []: 5540845445
        Work Phone []: 5544559854
        Home Phone []: 59854678
        Other []:
ette information est-elle correcte ? [O/n]o
```

Une fois l'utilisateur crée on fait :

Et on fait cette commande

```
root@debian-ssh:~# nano /etc/ssh/sshd_config
```

Pour modifier le fichier pour que l'utilisateur peut se connecter en ssh

```
#       $OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

On recherche le AllowUsers, mais ici on ne le voit pas donc on va l'ajouter comme ceci :

```
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
AllowUsers john

#PubkeyAuthentication yes
```

Et aussi pour autoriser la connexion avec mdp on enlève le # de PasswordAuthentication pour que la ligne ne soit plus commenter

```
  GNU nano 5.4                    /etc/ssh/sshd_config *
# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile     .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hos
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication yes
```

Une fois cela fait on sauvegarde avec CTRL+X et on confirme avec o
puis on redémarre le service ssh

```
root@debian-ssh:~# sudo service ssh restart
```

Ensuite on effectue cette commande :

```
root@debian-ssh:~# sudo netstat -tlnp | grep ssh
```

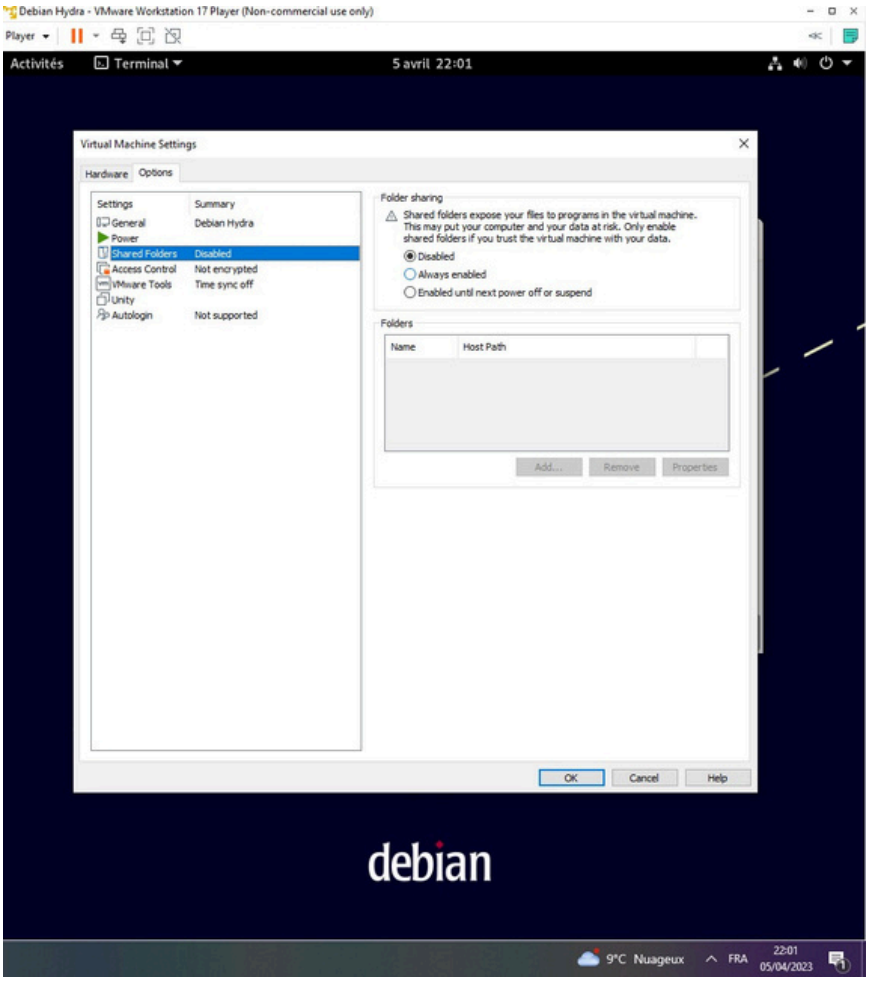
Et on voit bien que le serveur ssh écoute le port 22

```
oot@debian-ssh:~# sudo netstat -tlnp | grep ssh
cp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
.686/sshd: /usr/sbi
cp6       0      0 :::22                   :::*                    LISTEN
.686/sshd: /usr/sbi
oot@debian-ssh:~#
```

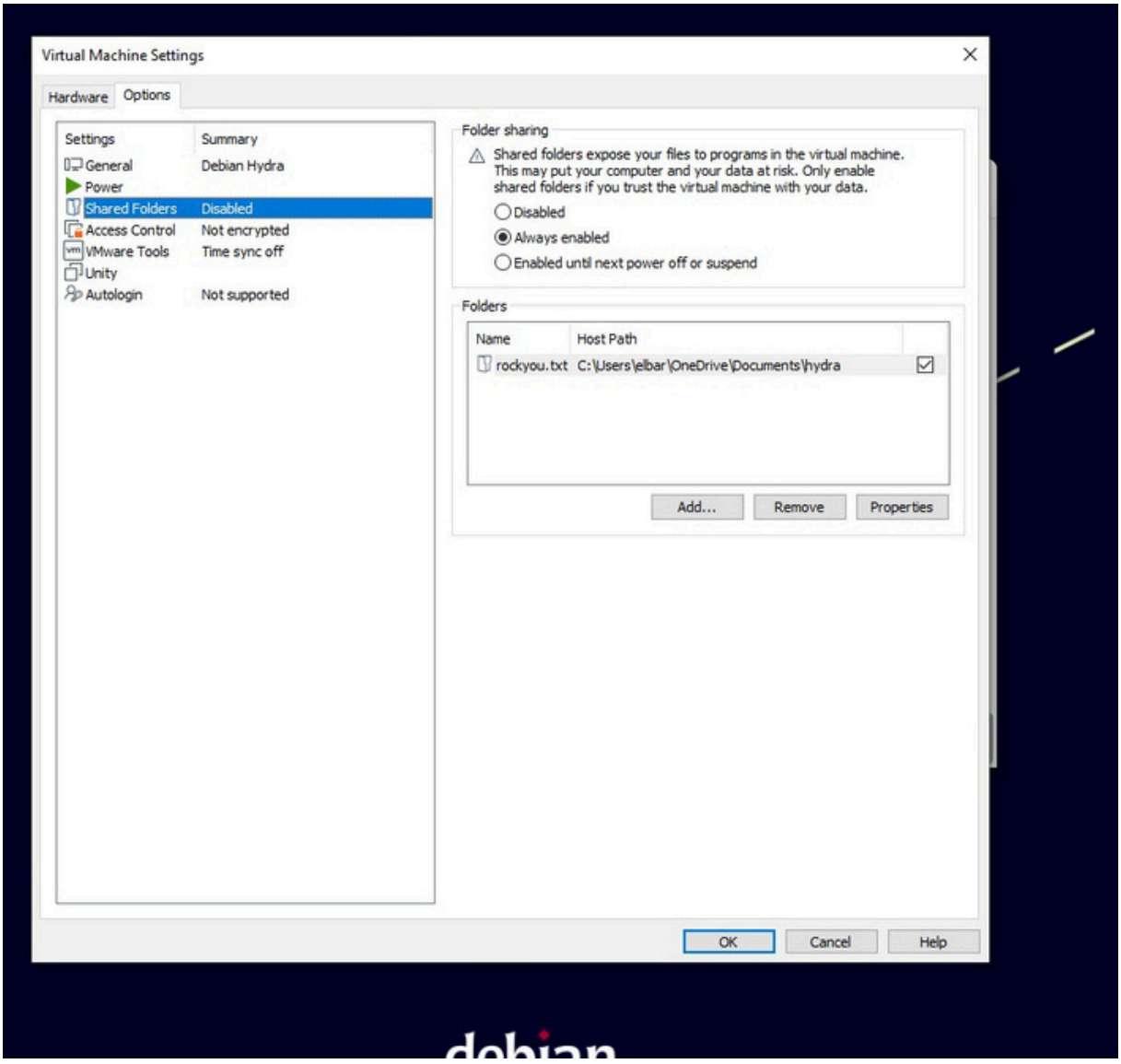
Sur la machine hydra maintenant, on va récupérer le dictionnaire de mdp grâce à la partage de la vm avant on vérifie si tout est bon pour faire le partage avec cette commande :

```
root@debian-hydra:~# sudo apt-get install open-vm-tools-desktop
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
open-vm-tools-desktop est déjà la version la plus récente (2:11.2.5-2+deb11u1).
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
```

Ensuite on va dans les paramètres de la vm et on va activer le partage de fichier :



Et on va renseigner ou se trouve notre fichier rockyou.txt



une fois cela fait on retourne sur la vm (toujours hydra)

On execute cette commande :

```
root@debian-hydra:~# vmware-hgfsclient
hydra
```

On voit bien notre dossier hydra est partager

Ensuite on fait :

```
root@debian-hydra:~# sudo mkdir /mnt/hgfs/hydra
```

Afin de crée le répertoire hydra

Maintenant on va partager le répertoire hydra avec :

Sudo vmhgfs-fuse .host/hydra /mnt/hgfs/hydra -o allow_other -o uid=1000

```
root@debian-hydra:~# sudo vmhgfs-fuse .host:/hydra /mnt/hgfs/hydra -o allow_othe
r -o uid=1000
```

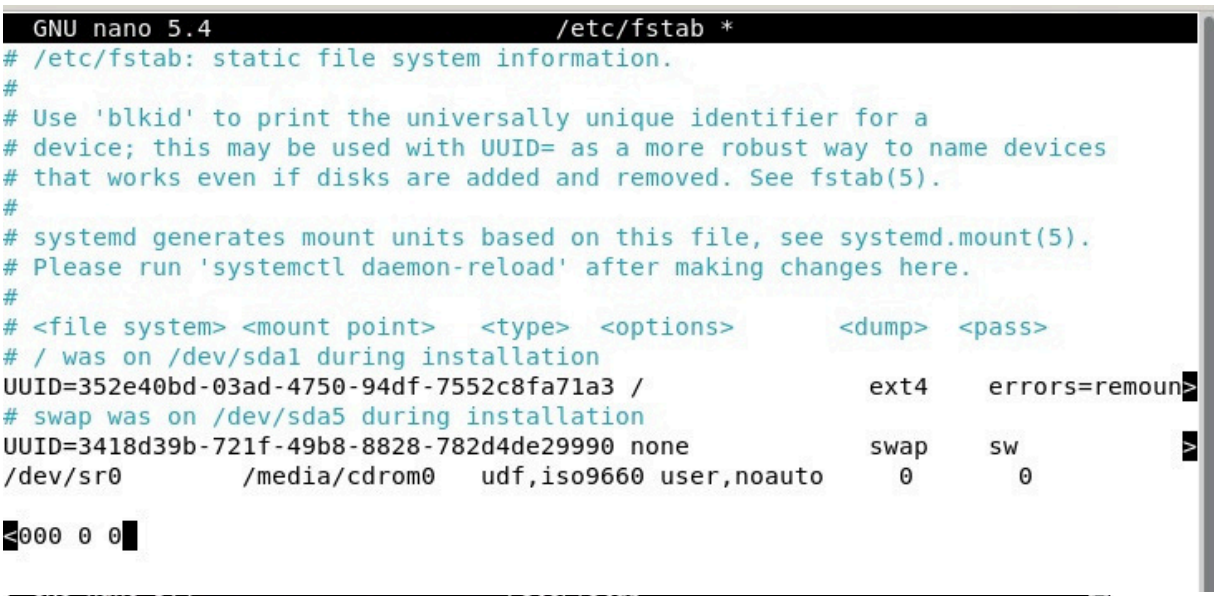
Ensuite on va se placer dans le dossier hydra

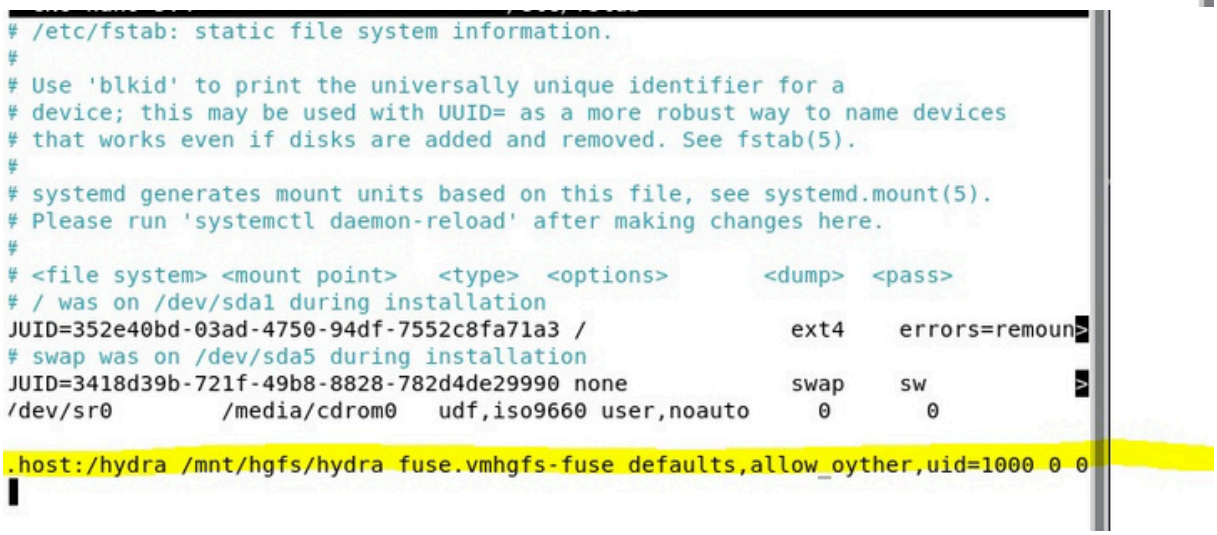
```
root@debian-hydra:~# cd /mnt/hgfs/hydra
root@debian-hydra:/mnt/hgfs/hydra# ls -lia
total 136647
2 drwxrwxrwx 1 root root         0  5 avril 22:03 .
1 dr-xr-xr-x 1 root root      4192  5 avril 22:18 ..
3 -rwxrwxrwx 1 root root 139921497  5 avril 22:02 rockyou.txt
```

Et comme on peut voir grâce à ls -lia on peut voir tous les fichiers dans le dossier dont le rockyou.txt

Pour maintenir le partage si on redémarre la vm on va dans

/etc/fstab avec nano
et on ajoute les dernières ligne qui sont sur le screen





Et on sauvegarde le fichier

On va enfin lancer l’attaque sur le sevreur ssh depuis la machine hydra grace à

```
root@debian-hydra:~# hydra -l john -P /usr/share/hydra/rockyou.txt ssh://192.168
.1.20
```

Attaque depuis la machine hydra :

```
root@debian-hydra:~# hydra -v -l john -P /mnt/hgfs/hydra/rockyou.txt ssh://192.168.1.20:22
Hydra v9.1 (c) 2020 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 2023-04-05 22:32:55
[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, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking ssh://192.168.1.20:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://john@192.168.1.20:22
[INFO] Successful, password authentication is supported by ssh://192.168.1.20:22
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
^C[ERROR] Received signal 2, going down ...
The session file ./hydra.restore was written. Type "hydra -R" to resume session.
root@debian-hydra:~# hydra -v -l john -P /mnt/hgfs/hydra/rockyou.txt ssh://192.168.1.20
Hydra v9.1 (c) 2020 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 2023-04-05 22:33:14
[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 previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking ssh://192.168.1.20:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://john@192.168.1.20:22
[INFO] Successful, password authentication is supported by ssh://192.168.1.20:22
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
^C[ERROR] Received signal 2, going down ...
The session file ./hydra.restore was written. Type "hydra -R" to resume session.
root@debian-hydra:~# hydra -v -l john -P /mnt/hgfs/hydra/rockyou.txt ssh://192.168.1.20
Hydra v9.1 (c) 2020 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 2023-04-05 22:36:55
[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 previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking ssh://192.168.1.20:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://john@192.168.1.20:22
[INFO] Successful, password authentication is supported by ssh://192.168.1.20:22
```

Ici on voit les logs du serveur SSH :

```
root@debian-ssh:~# tail -f /var/log/auth.log
Apr  5 22:33:44 debian-ssh sshd[1831]: Disconnecting invalid user john 192.168.1.30 port 39542: Too many authentication failures [preauth]
Apr  5 22:33:44 debian-ssh sshd[1831]: PAM 5 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.30
Apr  5 22:33:44 debian-ssh sshd[1831]: PAM service(sshd) ignoring max retries; 6 > 3
Apr  5 22:34:52 debian-ssh gdm-password]: gkr-pam: unlocked login keyring
Apr  5 22:35:10 debian-ssh sudo:     root : TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/usr/bin/tail -f/var/log/auth.log
Apr  5 22:35:10 debian-ssh sudo: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=0)
Apr  5 22:35:10 debian-ssh sudo: pam_unix(sudo:session): session closed for user root
Apr  5 22:35:22 debian-ssh sudo:     root : TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/usr/bin/tail -f/var/log/auth.log
Apr  5 22:35:22 debian-ssh sudo: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=0)
Apr  5 22:35:22 debian-ssh sudo: pam_unix(sudo:session): session closed for user root
Apr  5 22:37:06 debian-ssh sshd[1701]: exited MaxStartups throttling after 00:03:40, 1 connections dropped
Apr  5 22:37:06 debian-ssh sshd[1865]: Invalid user john from 192.168.1.30 port 34494
Apr  5 22:37:06 debian-ssh sshd[1865]: Received disconnect from 192.168.1.30 port 34494:11: Bye Bye [preauth]
Apr  5 22:37:06 debian-ssh sshd[1865]: Disconnected from invalid user john 192.168.1.30 port 34494 [preauth]
Apr  5 22:37:06 debian-ssh sshd[1701]: error: beginning MaxStartups throttling
Apr  5 22:37:06 debian-ssh sshd[1701]: drop connection #11 from [192.168.1.30]:34598 on [192.168.1.20]:22 past MaxStartups
Apr  5 22:37:07 debian-ssh sshd[1873]: Invalid user john from 192.168.1.30 port 34558
Apr  5 22:37:07 debian-ssh sshd[1872]: Invalid user john from 192.168.1.30 port 34550
Apr  5 22:37:07 debian-ssh sshd[1875]: Invalid user john from 192.168.1.30 port 34584
Apr  5 22:37:07 debian-ssh sshd[1871]: Invalid user john from 192.168.1.30 port 34540
Apr  5 22:37:07 debian-ssh sshd[1873]: pam_unix(sshd:auth): check pass; user unknown
Apr  5 22:37:07 debian-ssh sshd[1873]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.30
Apr  5 22:37:07 debian-ssh sshd[1872]: pam_unix(sshd:auth): check pass; user unknown
Apr  5 22:37:07 debian-ssh sshd[1872]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.30
Apr  5 22:37:07 debian-ssh sshd[1875]: pam_unix(sshd:auth): check pass; user unknown
Apr  5 22:37:07 debian-ssh sshd[1875]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.30
Apr  5 22:37:07 debian-ssh sshd[1871]: pam_unix(sshd:auth): check pass; user unknown
Apr  5 22:37:07 debian-ssh sshd[1871]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.30
Apr  5 22:37:07 debian-ssh sshd[1876]: Invalid user john from 192.168.1.30 port 34588
Apr  5 22:37:07 debian-ssh sshd[1870]: Invalid user john from 192.168.1.30 port 34538
Apr  5 22:37:07 debian-ssh sshd[1877]: Invalid user john from 192.168.1.30 port 34592
Apr  5 22:37:07 debian-ssh sshd[1869]: Invalid user john from 192.168.1.30 port 34522
Apr  5 22:37:07 debian-ssh sshd[1870]: pam_unix(sshd:auth): check pass; user unknown
Apr  5 22:37:07 debian-ssh sshd[1870]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.30
Apr  5 22:37:07 debian-ssh sshd[1874]: Invalid user john from 192.168.1.30 port 34574
Apr  5 22:37:07 debian-ssh sshd[1869]: pam_unix(sshd:auth): check pass; user unknown
Apr  5 22:37:07 debian-ssh sshd[1877]: pam_unix(sshd:auth): check pass; user unknown
Apr  5 22:37:07 debian-ssh sshd[1877]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.30
Apr  5 22:37:07 debian-ssh sshd[1868]: Invalid user john from 192.168.1.30 port 34514
```

Les logs de la machine rsyslog qui sont donc bien centraliser :

```
root@debian-Ryslog:~# tail -f /var/log/auth.log
Apr  5 22:33:44 debian-ssh sshd[1831]: Disconnecting invalid user john 192.168.1.30 port 39542: Too many authentication failures [preauth]
Apr  5 22:33:44 debian-ssh sshd[1831]: PAM 5 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.30
Apr  5 22:33:44 debian-ssh sshd[1831]: PAM service(sshd) ignoring max retries; 6 > 3
Apr  5 22:34:52 debian-ssh gdm-password]: gkr-pam: unlocked login keyring
Apr  5 22:35:10 debian-ssh sudo:     root : TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/usr/bin/tail -f/var/log/auth.log
Apr  5 22:35:10 debian-ssh sudo: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=0)
Apr  5 22:35:10 debian-ssh sudo: pam_unix(sudo:session): session closed for user root
Apr  5 22:35:22 debian-ssh sudo:     root : TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/usr/bin/tail -f/var/log/auth.log
Apr  5 22:35:22 debian-ssh sudo: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=0)
Apr  5 22:35:22 debian-ssh sudo: pam_unix(sudo:session): session closed for user root
Apr  5 22:37:06 debian-ssh sshd[1701]: exited MaxStartups throttling after 00:03:40, 1 connections dropped
Apr  5 22:37:06 debian-ssh sshd[1865]: Invalid user john from 192.168.1.30 port 34494
Apr  5 22:37:06 debian-ssh sshd[1865]: Received disconnect from 192.168.1.30 port 34494:11: Bye Bye [preauth]
Apr  5 22:37:06 debian-ssh sshd[1865]: Disconnected from invalid user john 192.168.1.30 port 34494 [preauth]
Apr  5 22:37:06 debian-ssh sshd[1701]: error: beginning MaxStartups throttling
Apr  5 22:37:06 debian-ssh sshd[1701]: drop connection #11 from [192.168.1.30]:34598 on [192.168.1.20]:22 past MaxStartups
Apr  5 22:37:07 debian-ssh sshd[1873]: Invalid user john from 192.168.1.30 port 34558
Apr  5 22:37:07 debian-ssh sshd[1872]: Invalid user john from 192.168.1.30 port 34550
Apr  5 22:37:07 debian-ssh sshd[1875]: Invalid user john from 192.168.1.30 port 34584
Apr  5 22:37:07 debian-ssh sshd[1871]: Invalid user john from 192.168.1.30 port 34540
Apr  5 22:37:07 debian-ssh sshd[1873]: pam_unix(sshd:auth): check pass; user unknown
Apr  5 22:37:07 debian-ssh sshd[1873]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.30
Apr  5 22:37:07 debian-ssh sshd[1872]: pam_unix(sshd:auth): check pass; user unknown
Apr  5 22:37:07 debian-ssh sshd[1872]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.30
Apr  5 22:37:07 debian-ssh sshd[1875]: pam_unix(sshd:auth): check pass; user unknown
Apr  5 22:37:07 debian-ssh sshd[1875]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.30
Apr  5 22:37:07 debian-ssh sshd[1871]: pam_unix(sshd:auth): check pass; user unknown
Apr  5 22:37:07 debian-ssh sshd[1871]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.30
Apr  5 22:37:07 debian-ssh sshd[1876]: Invalid user john from 192.168.1.30 port 34588
Apr  5 22:37:07 debian-ssh sshd[1870]: Invalid user john from 192.168.1.30 port 34538
Apr  5 22:37:07 debian-ssh sshd[1877]: Invalid user john from 192.168.1.30 port 34592
Apr  5 22:37:07 debian-ssh sshd[1869]: Invalid user john from 192.168.1.30 port 34522
Apr  5 22:37:07 debian-ssh sshd[1870]: pam_unix(sshd:auth): check pass; user unknown
Apr  5 22:37:07 debian-ssh sshd[1870]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.30
Apr  5 22:37:07 debian-ssh sshd[1874]: Invalid user john from 192.168.1.30 port 34574
```

4-Analyse des logs :

-On voit bien l’adresse ip de l’attaquant, et les mots de passe qu’il a essayer :

```
root@debian-Ryslog:~# tail -f /var/log/auth.log
Apr  5 22:33:44 debian-ssh sshd[1831]: Disconnecting invalid user john 192.168.1.30 port 39542: Too many authentication failures [preauth]
Apr  5 22:33:44 debian-ssh sshd[1831]: PAM 5 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.30
Apr  5 22:33:44 debian-ssh sshd[1831]: PAM service(sshd) ignoring max retries; 6 > 3
Apr  5 22:34:52 debian-ssh gdm-password]: gkr-pam: unlocked login keyring
Apr  5 22:35:10 debian-ssh sudo:     root : TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/usr/bin/tail -f/var/log/auth.log
Apr  5 22:35:10 debian-ssh sudo: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=0)
Apr  5 22:35:10 debian-ssh sudo: pam_unix(sudo:session): session closed for user root
Apr  5 22:35:22 debian-ssh sudo:     root : TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/usr/bin/tail -f/var/log/auth.log
Apr  5 22:35:22 debian-ssh sudo: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=0)
Apr  5 22:35:22 debian-ssh sudo: pam_unix(sudo:session): session closed for user root
Apr  5 22:37:06 debian-ssh sshd[1701]: exited MaxStartups throttling after 00:03:40, 1 connections dropped
Apr  5 22:37:06 debian-ssh sshd[1865]: Invalid user john from 192.168.1.30 port 34494
Apr  5 22:37:06 debian-ssh sshd[1865]: Received disconnect from 192.168.1.30 port 34494:11: Bye Bye [preauth]
Apr  5 22:37:06 debian-ssh sshd[1865]: Disconnected from invalid user john 192.168.1.30 port 34494 [preauth]
Apr  5 22:37:06 debian-ssh sshd[1701]: error: beginning MaxStartups throttling
Apr  5 22:37:06 debian-ssh sshd[1701]: drop connection #11 from [192.168.1.30]:34598 on [192.168.1.20]:22 past MaxStartups
Apr  5 22:37:07 debian-ssh sshd[1873]: Invalid user john from 192.168.1.30 port 34558
Apr  5 22:37:07 debian-ssh sshd[1872]: Invalid user john from 192.168.1.30 port 34550
Apr  5 22:37:07 debian-ssh sshd[1875]: Invalid user john from 192.168.1.30 port 34584
Apr  5 22:37:07 debian-ssh sshd[1871]: Invalid user john from 192.168.1.30 port 34540
Apr  5 22:37:07 debian-ssh sshd[1873]: pam_unix(sshd:auth): check pass; user unknown
Apr  5 22:37:07 debian-ssh sshd[1873]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.30
Apr  5 22:37:07 debian-ssh sshd[1872]: pam_unix(sshd:auth): check pass; user unknown
Apr  5 22:37:07 debian-ssh sshd[1872]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.30
Apr  5 22:37:07 debian-ssh sshd[1875]: pam_unix(sshd:auth): check pass; user unknown
Apr  5 22:37:07 debian-ssh sshd[1875]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.30
Apr  5 22:37:07 debian-ssh sshd[1871]: pam_unix(sshd:auth): check pass; user unknown
Apr  5 22:37:07 debian-ssh sshd[1871]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.30
Apr  5 22:37:07 debian-ssh sshd[1876]: Invalid user john from 192.168.1.30 port 34588
Apr  5 22:37:07 debian-ssh sshd[1870]: Invalid user john from 192.168.1.30 port 34538
Apr  5 22:37:07 debian-ssh sshd[1877]: Invalid user john from 192.168.1.30 port 34592
Apr  5 22:37:07 debian-ssh sshd[1869]: Invalid user john from 192.168.1.30 port 34522
Apr  5 22:37:07 debian-ssh sshd[1870]: pam_unix(sshd:auth): check pass; user unknown
Apr  5 22:37:07 debian-ssh sshd[1870]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.30
Apr  5 22:37:07 debian-ssh sshd[1874]: Invalid user john from 192.168.1.30 port 34574
```

Ainsi que les tentatives de connexion par force brute

Et aussi toute les tentatives rater :

```
Apr  5 22:44:06 debian-ssh sshd[1935]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rho
Apr  5 22:44:07 debian-ssh sshd[1911]: Failed password for johndoe from 192.168.1.30 port 56718 ssh2
Apr  5 22:44:07 debian-ssh sshd[1908]: Failed password for johndoe from 192.168.1.30 port 56684 ssh2
Apr  5 22:44:07 debian-ssh sshd[1906]: Failed password for johndoe from 192.168.1.30 port 56676 ssh2
Apr  5 22:44:07 debian-ssh sshd[1912]: Failed password for johndoe from 192.168.1.30 port 56722 ssh2
Apr  5 22:44:07 debian-ssh sshd[1913]: Failed password for johndoe from 192.168.1.30 port 56738 ssh2
Apr  5 22:44:07 debian-ssh sshd[1918]: Failed password for johndoe from 192.168.1.30 port 56788 ssh2
Apr  5 22:44:07 debian-ssh sshd[1917]: Failed password for johndoe from 192.168.1.30 port 56784 ssh2
Apr  5 22:44:07 debian-ssh sshd[1914]: Failed password for johndoe from 192.168.1.30 port 56752 ssh2
Apr  5 22:44:07 debian-ssh sshd[1916]: Failed password for johndoe from 192.168.1.30 port 56772 ssh2
Apr  5 22:44:07 debian-ssh sshd[1907]: Failed password for johndoe from 192.168.1.30 port 56682 ssh2
Apr  5 22:44:07 debian-ssh sshd[1909]: Failed password for johndoe from 192.168.1.30 port 56700 ssh2
Apr  5 22:44:08 debian-ssh sshd[1910]: Failed password for johndoe from 192.168.1.30 port 56702 ssh2
Apr  5 22:44:08 debian-ssh sshd[1905]: Failed password for johndoe from 192.168.1.30 port 56664 ssh2
Apr  5 22:44:08 debian-ssh sshd[1919]: Failed password for johndoe from 192.168.1.30 port 56818 ssh2
Apr  5 22:44:08 debian-ssh sshd[1915]: Failed password for johndoe from 192.168.1.30 port 56762 ssh2
Apr  5 22:44:08 debian-ssh sshd[1935]: Failed password for johndoe from 192.168.1.30 port 56830 ssh2
Apr  5 22:44:09 debian-ssh sshd[1911]: Failed password for johndoe from 192.168.1.30 port 56718 ssh2
Apr  5 22:44:09 debian-ssh sshd[1912]: Failed password for johndoe from 192.168.1.30 port 56722 ssh2
Apr  5 22:44:10 debian-ssh sshd[1907]: Failed password for johndoe from 192.168.1.30 port 56682 ssh2
Apr  5 22:44:10 debian-ssh sshd[1913]: Failed password for johndoe from 192.168.1.30 port 56738 ssh2
Apr  5 22:44:10 debian-ssh sshd[1908]: Failed password for johndoe from 192.168.1.30 port 56684 ssh2
Apr  5 22:44:10 debian-ssh sshd[1914]: Failed password for johndoe from 192.168.1.30 port 56752 ssh2
Apr  5 22:44:10 debian-ssh sshd[1910]: Failed password for johndoe from 192.168.1.30 port 56702 ssh2
Apr  5 22:44:10 debian-ssh sshd[1909]: Failed password for johndoe from 192.168.1.30 port 56700 ssh2
Apr  5 22:44:10 debian-ssh sshd[1906]: Failed password for johndoe from 192.168.1.30 port 56676 ssh2
Apr  5 22:44:10 debian-ssh sshd[1905]: Failed password for johndoe from 192.168.1.30 port 56664 ssh2
Apr  5 22:44:10 debian-ssh sshd[1918]: Failed password for johndoe from 192.168.1.30 port 56788 ssh2
Apr  5 22:44:10 debian-ssh sshd[1916]: Failed password for johndoe from 192.168.1.30 port 56772 ssh2
Apr  5 22:44:10 debian-ssh sshd[1917]: Failed password for johndoe from 192.168.1.30 port 56784 ssh2
Apr  5 22:44:10 debian-ssh sshd[1915]: Failed password for johndoe from 192.168.1.30 port 56762 ssh2
Apr  5 22:44:10 debian-ssh sshd[1919]: Failed password for johndoe from 192.168.1.30 port 56818 ssh2
Apr  5 22:44:10 debian-ssh sshd[1935]: Failed password for johndoe from 192.168.1.30 port 56830 ssh2
Apr  5 22:44:13 debian-ssh sshd[1911]: Failed password for johndoe from 192.168.1.30 port 56718 ssh2
Apr  5 22:44:13 debian-ssh sshd[1912]: Failed password for johndoe from 192.168.1.30 port 56722 ssh2
Apr  5 22:44:13 debian-ssh sshd[1907]: Failed password for johndoe from 192.168.1.30 port 56682 ssh2
Apr  5 22:44:13 debian-ssh sshd[1909]: Failed password for johndoe from 192.168.1.30 port 56700 ssh2
```

5-

- Discuter de l'importance de la centralisation des logs pour la détection des attaques

  -La centralisation des logs est importantes puisque grace à celle-ci on peut savoir ce qu'il se passe sur les différents poste, et donc détecter une potentielle menace, et de l'identifier afin de la neutraliser et de savoir quand elle se produit, la centralisation des logs va permettre aussi la surveillance continue des poste de travail. La centralisation des logs pour la détection des attaques est importantes puique on pouura surveiller efficacement le systèmes et donc détecter les menaces et les tentatives de connexion.

- Discuter des mesures de sécurité pour prévenir les attaques brute force sur le serveur SSH

  -Le serveur va deconnecter l'attaquant au bout d'un certains nombres de mot de passe échouer
  -SI on tente trop de connexion on ne pourra plus se connecter du tout au service
  -Il va donc arreter le service afin que l'attaquant ne puisse plus accèder au serveur SSH
  Le serveur SSH n'est pas totalement sécuriser car si l'attaquant arrive à se connecter alors les services ne seront pas arreter et l'attaquant pourra faire ce qu'il veut sur le compte pirater, il faudrait rajouter d'autres mesures de sécurité comme le blocage d'ip après un certain
  nombre d'erreurs.

6-

On va installer fail2ban

```
root@debian-ssh:~# apt-get install fail2ban
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  python3-pyinotify python3-systemd whois
Paquets suggérés :
  mailx monit sqlite3 python-pyinotify-doc
Les NOUVEAUX paquets suivants seront installés :
  fail2ban python3-pyinotify python3-systemd whois
0 mis à jour, 4 nouvellement installés, 0 à enlever et 3 non mis à jour.
Il est nécessaire de prendre 596 ko dans les archives.
Après cette opération, 2 819 ko d'espace disque supplémentaires seront util
Souhaitez-vous continuer ? [O/n] o
Réception de :1 http://deb.debian.org/debian bullseye/main amd64 fail2ban a
11.2-2 [451 kB]
Réception de :2 http://deb.debian.org/debian bullseye/main amd64 python3-py
fy all 0.9.6-1.3 [27,2 kB]
Réception de :3 http://deb.debian.org/debian bullseye/main amd64 python3-sy
 amd64 234-3+b4 [36,4 kB]
Réception de :4 http://deb.debian.org/debian bullseye/main amd64 whois amd6
```

Une fois fail2ban installer on fait cette comande :

```
root@debian-ssh:~# sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
```

Qui va crée un fichier de configuration pour fail2ban

Ensuite on fait sudo nano /etc/fail2ban/jail.local

```
  GNU nano 5.4                /etc/fail2ban/jail.local *
#
# YOU SHOULD NOT MODIFY THIS FILE.
#
# It will probably be overwritten or improved in a distribution update.
#
# Provide customizations in a jail.local file or a jail.d/customisation.local.
# For example to change the default bantime for all jails and to enable the
# ssh-iptables jail the following (uncommented) would appear in the .local file.
# See man 5 jail.conf for details.
#
# [DEFAULT]
# bantime = 1h
#
# [sshd]
 enabled = true
port=ssh
filter =sshd
logpath = /var/log/rsyslog/ssh.log
maxretry=3
```

Une fois dans le fichier on ajoute tout ce qu'il y a après le [sshd]
et on sauvegarde le fichier

Et grâce à fail2ban l'attaquant ne pourra plus se connecter après trois tentative