```
maxime2@debian:~$ sudo apt install -y rsyslog
[sudo] Mot de passe de maxime2 :
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
rsyslog est déjà la version la plus récente (8.2102
.0-2+deb11u1).
```

```
maxime2@debian:~$ sudo systemctl status rsyslog
● rsyslog.service - System Logging Service
     Loaded: loaded (/lib/systemd/system/rsyslog.s>
     Active: active (running) since Thu 2024-04-04>
TriggeredBy: ● syslog.socket
       Docs: man:rsyslogd(8)
             man:rsyslog.conf(5)
             https://www.rsyslog.com/doc/
   Main PID: 395 (rsyslogd)
      Tasks: 4 (limit: 2306)
     Memory: 2.9M
        CPU: 86ms
     CGroup: /system.slice/rsyslog.service
             └─395 /usr/sbin/rsyslogd -n -iNONE

avril 04 16:31:43 debian systemd[1]: Starting Syst>
avril 04 16:31:43 debian rsyslogd[395]: imuxsock: >
avril 04 16:31:43 debian rsyslogd[395]: [origin so>
avril 04 16:31:43 debian systemd[1]: Started Syste>
lines 1-18/18 (END)
```

```
maxime2@debian:~$ sudo vi /etc/rsyslog.conf
```

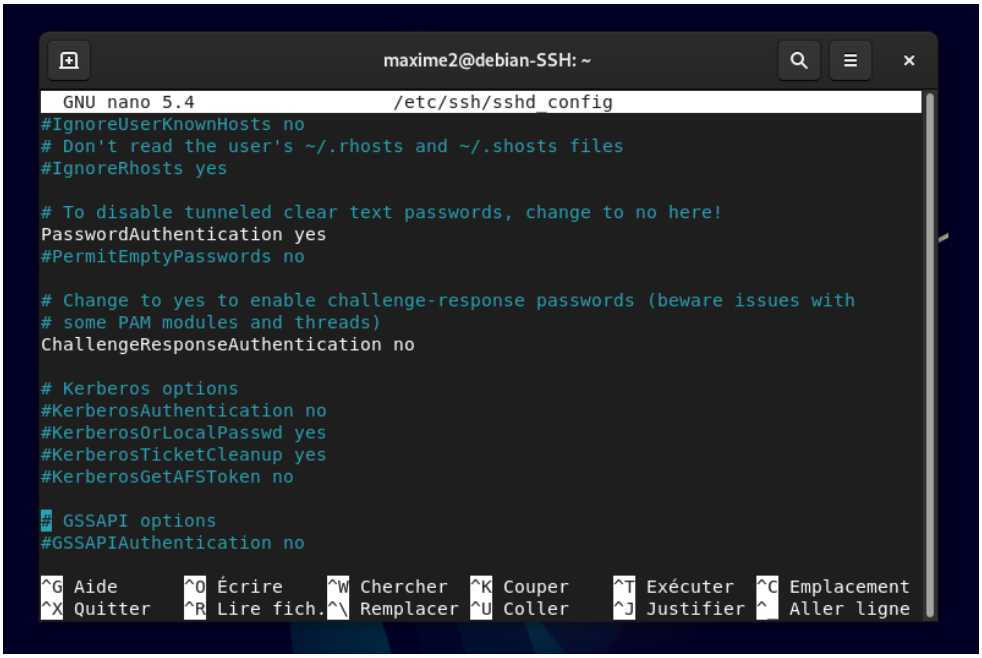
```
module(load="imuxsock") # provides support for loc>
module(load="imklog")   # provides kernel logging >
#module(load="immark")  # provides --MARK-- messag>

# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")

$template remote-incoming-logs,"/var/log/%HOSTNAM/>
*.* ?remote-incoming-logs
```

```
maxime2@debian-Rsyslog:~$ sudo netstat -lnup
Connexions Internet actives (seulement serveurs)
Proto Recv-Q Send-Q Adresse locale          Adresse distante        Etat
PID/Program name
udp        0      0 0.0.0.0:5353            0.0.0.0:*
348/avahi-daemon: r
udp        0      0 0.0.0.0:631             0.0.0.0:*
492/cups-browsed
udp        0      0 0.0.0.0:57267           0.0.0.0:*
348/avahi-daemon: r
udp6       0      0 :::5353                 :::*
348/avahi-daemon: r
udp6       0      0 :::50162                :::*
348/avahi-daemon: r
```

```
maxime2@debian-SSH:~$ sudo apt install openssh-client
[sudo] Mot de passe de maxime2 :
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
openssh-client est déjà la version la plus récente (1:8.4p1-5+deb11u3).
Les paquets suivants ont été installés automatiquement et ne sont plus néc
```

```
maxime2@debian-SSH:~$ sudo apt 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+deb11u3).
openssh-server passé en « installé manuellement ».
Les paquets suivants ont été installés automatiquement et ne sont plus nécessair
es :
  gyp libc-ares2 libjs-highlight.js libjs-inherits libjs-is-typedarray
```

```
maxime2@debian-SSH:~$ sudo editor /etc/ssh/sshd_config
```



```
maxime2@debian-SSH:~$ sudo netstat -tuln | grep 22
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
```

```
maxime2@debian-SSH:~$ sudo adduser userssh
Ajout de l'utilisateur « userssh » ...
Ajout du nouveau groupe « userssh » (1003) ...
Ajout du nouvel utilisateur « userssh » (1003) avec le groupe « userssh » ...
Création du répertoire personnel « /home/userssh »...
Copie des fichiers depuis « /etc/skel »...
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd: password updated successfully
Changing the user information for userssh
Enter the new value, or press ENTER for the default
        Full Name []: User
        Room Number []: 1
        Work Phone []:
        Home Phone []:
        Other []:
Cette information est-elle correcte ? [O/n]o
```

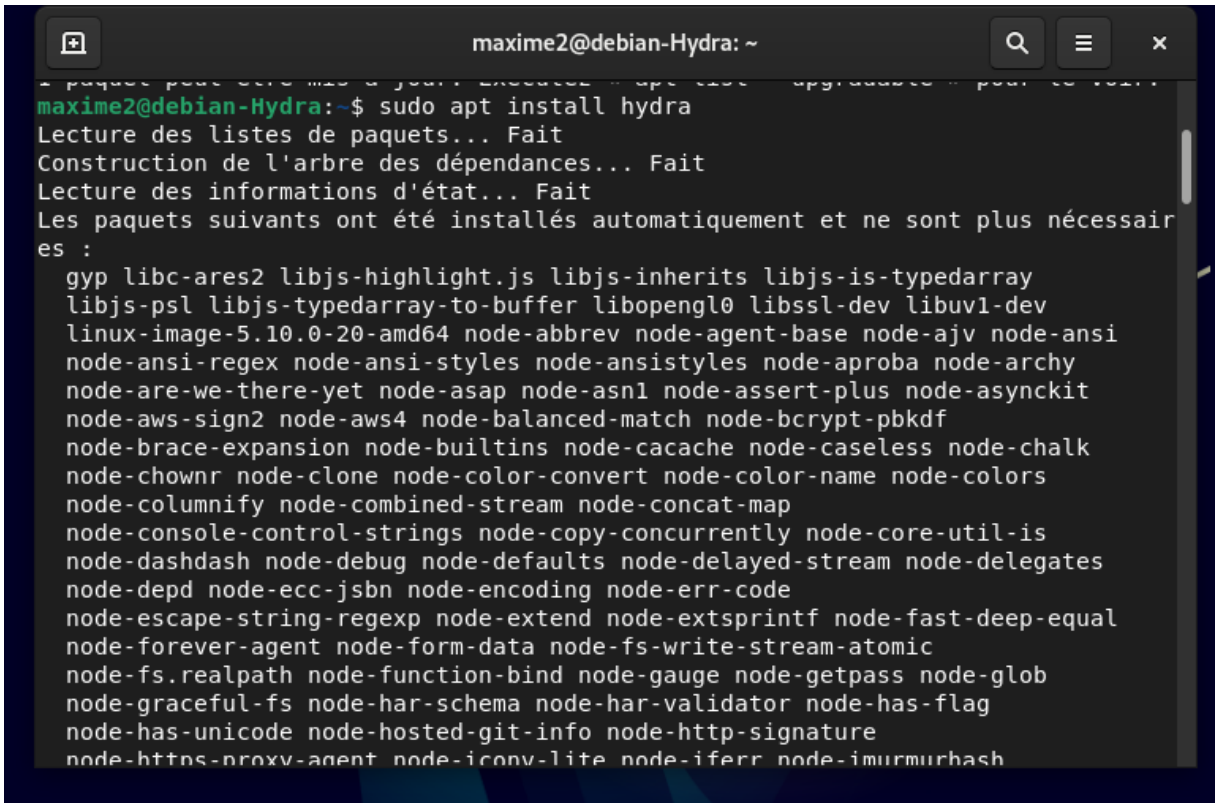
```
maxime2@debian-SSH:~$ sudo nano /etc/ssh/sshd config
```

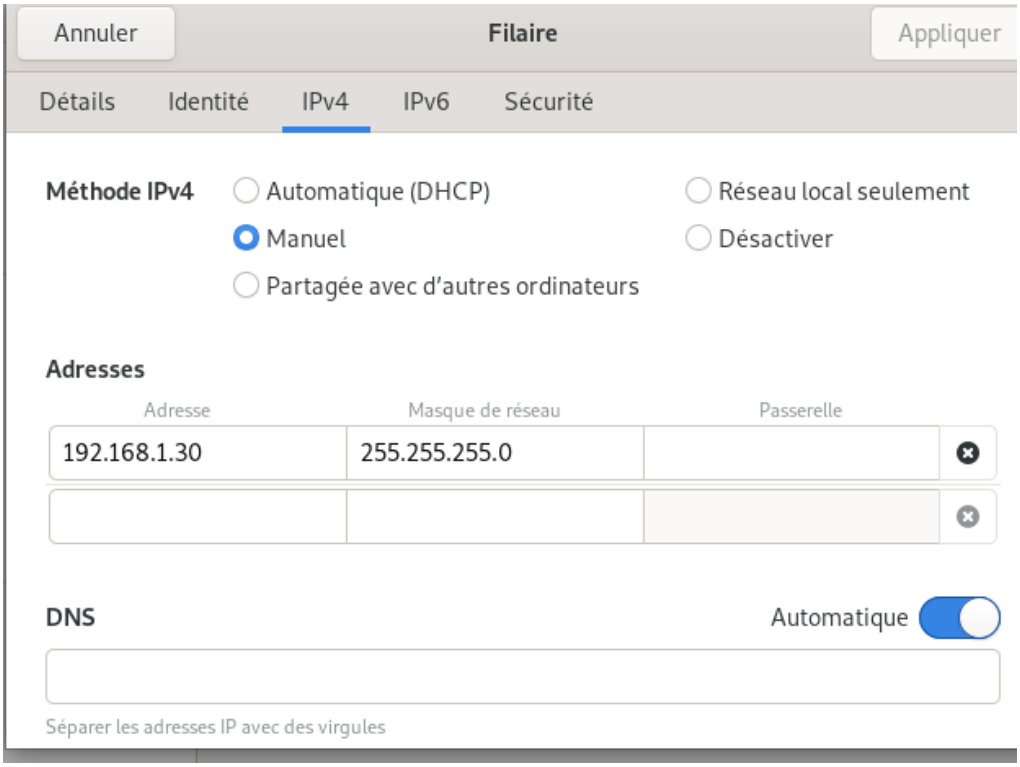
maxime2@debian-SSH: ~

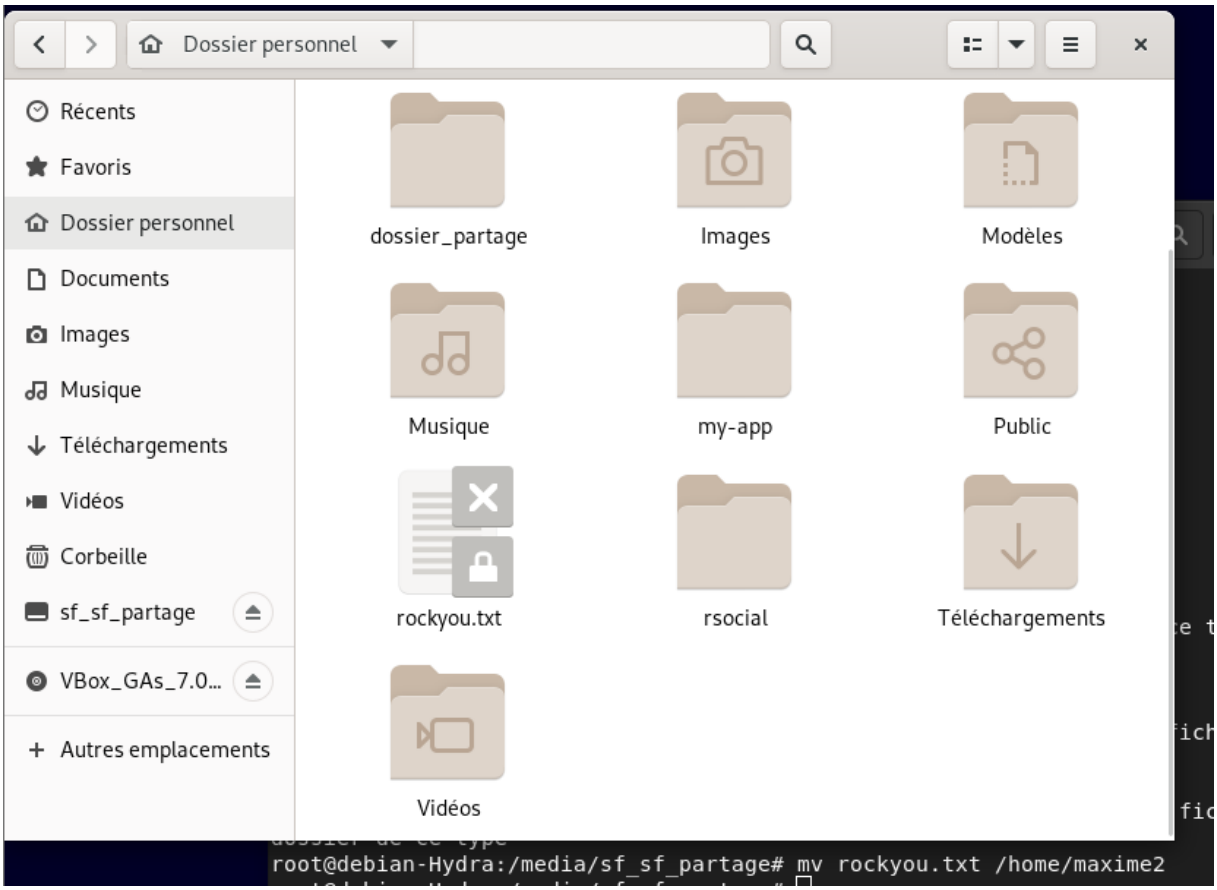
```
  GNU nano 5.4                    /etc/ssh/sshd_config
#ChrootDirectory none
#VersionAddendum none

# no default banner path
#Banner none

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# override default of no subsystems
Subsystem       sftp    /usr/lib/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#       X11Forwarding no
#       AllowTcpForwarding no
#       PermitTTY no
#       ForceCommand cvs server
AllowUsers userssh


^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^T Exécuter  ^C Emplacement
^X Quitter   ^R Lire fich.^\ Remplacer ^U Coller    ^J Justifier ^_ Aller ligne
```

```
maxime2@debian-SSH:~$ sudo service ssh restart
```

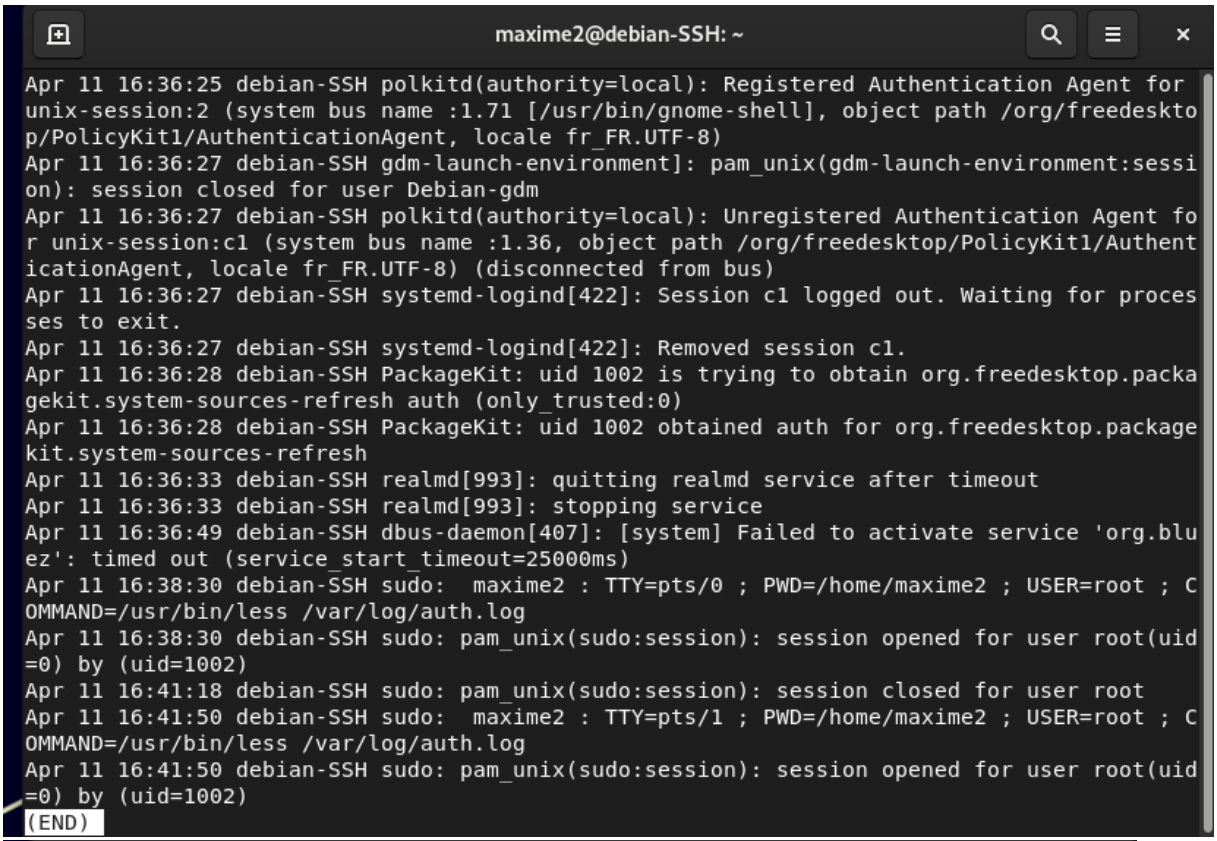
3- Machine Hydra

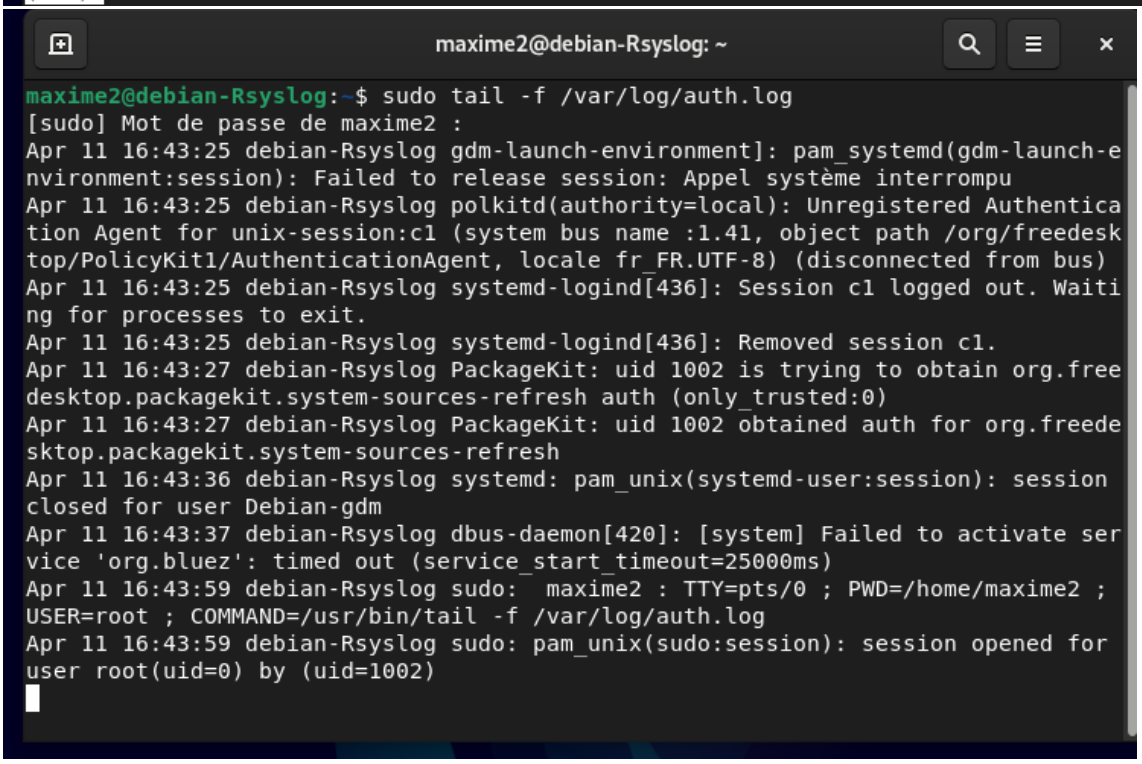







```
maxime2@debian-Hydra:~$ hydra -l userssh -P /home/maxime2 ssh://192.168.1.20
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in mi
litary or secret service organizations, or for illegal purposes (this is non-bin
ding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-11 16:37:
09
[WARNING] Many SSH configurations limit the number of parallel tasks, it is reco
mmended to reduce the tasks: use -t 4
```





Je n'ai pas réussi à régler le problème rencontré en cours, j'ai vérifié que toutes les machines avaient bien le port 22 ouvert mais la debian attaquante s'arrête toujours pendant l'attaque et je ne vois pas l'attaque dans les logs centralisés. Toutes les machines ont bien l'ip adéquate, les ports ouverts, sont sur le réseau interne, devant travailler le week-end et le bts blanc à réviser, je n'ai pas eu plus de temps pour recommencer tout le tp.

5 – Conclusion

Il est important de centraliser les logs pour mieux détecter les attaques et les analyser. On peut plus facilement voir les informations sur les attaques que si on devait parcourir tous les logs pour voir ceux qui concernent les attaques.

On doit protéger le SSH des attaques brute force en implantant des mots de passe forts, en verrouillant les comptes si il y a trop de tentatives de connexions infructueuses, on peut aussi utiliser une double authentification.