

```
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 nécessaires :
```

```
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 nécessaires :
```

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

```
maxime2@debian-SSH: ~
GNU nano 5.4 /etc/ssh/sshd config
#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
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no

# GSSAPI options
#GSSAPIAuthentication no

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

```
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 usersssh
Ajout de l'utilisateur « usersssh » ...
Ajout du nouveau groupe « usersssh » (1003) ...
Ajout du nouvel utilisateur « usersssh » (1003) avec le groupe « usersssh » ...
Création du répertoire personnel « /home/usersssh »...
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 usersssh
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 ? [0/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 usersssh

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

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

3- Machine Hydra

```
maxime2@debian-Hydra: ~$ sudo apt install hydra
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
gyp libc-ares2 libjs-highlight.js libjs-inherits libjs-is-typedarray
libjs-psl libjs-typedarray-to-buffer libopengl0 libssl-dev libuv1-dev
linux-image-5.10.0-20-amd64 node-abbrev node-agent-base node-ajv node-ansi
node-ansi-regex node-ansi-styles node-ansistyles node-aproba node-archy
node-are-we-there-yet node-asap node-asn1 node-assert-plus node-asynckit
node-aws-sign2 node-aws4 node-balanced-match node-bcrypt-pbkdf
node-brace-expansion node-builtins node-cacache node-caseless node-chalk
node-chownr node-clone node-color-convert node-color-name node-colors
node-columnify node-combined-stream node-concat-map
node-console-control-strings node-copy-concurrently node-core-util-is
node-dashdash node-debug node-defaults node-delayed-stream node-delegates
node-depd node-ecc-jsbn node-encoding node-err-code
node-escape-string-regexp node-extend node-extends node-fast-deep-equal
node-forever-agent node-form-data node-fs-write-stream-atomic
node-fs.realpath node-function-bind node-gauge node-getpass node-glob
node-graceful-fs node-har-schema node-har-validator node-has-flag
node-has-unicode node-hosted-git-info node-http-signature
node-https-proxy-agent node-iconv-lite node-iferr node-imurmurhash
```

Annuler

Filaire

Appliquer

Détails

Identité

IPv4

IPv6

Sécurité

Méthode IPv4

☐ Automatique (DHCP)

☐ Réseau local seulement

☒ Manuel

☐ Désactiver

☐ Partagée avec d'autres ordinateurs

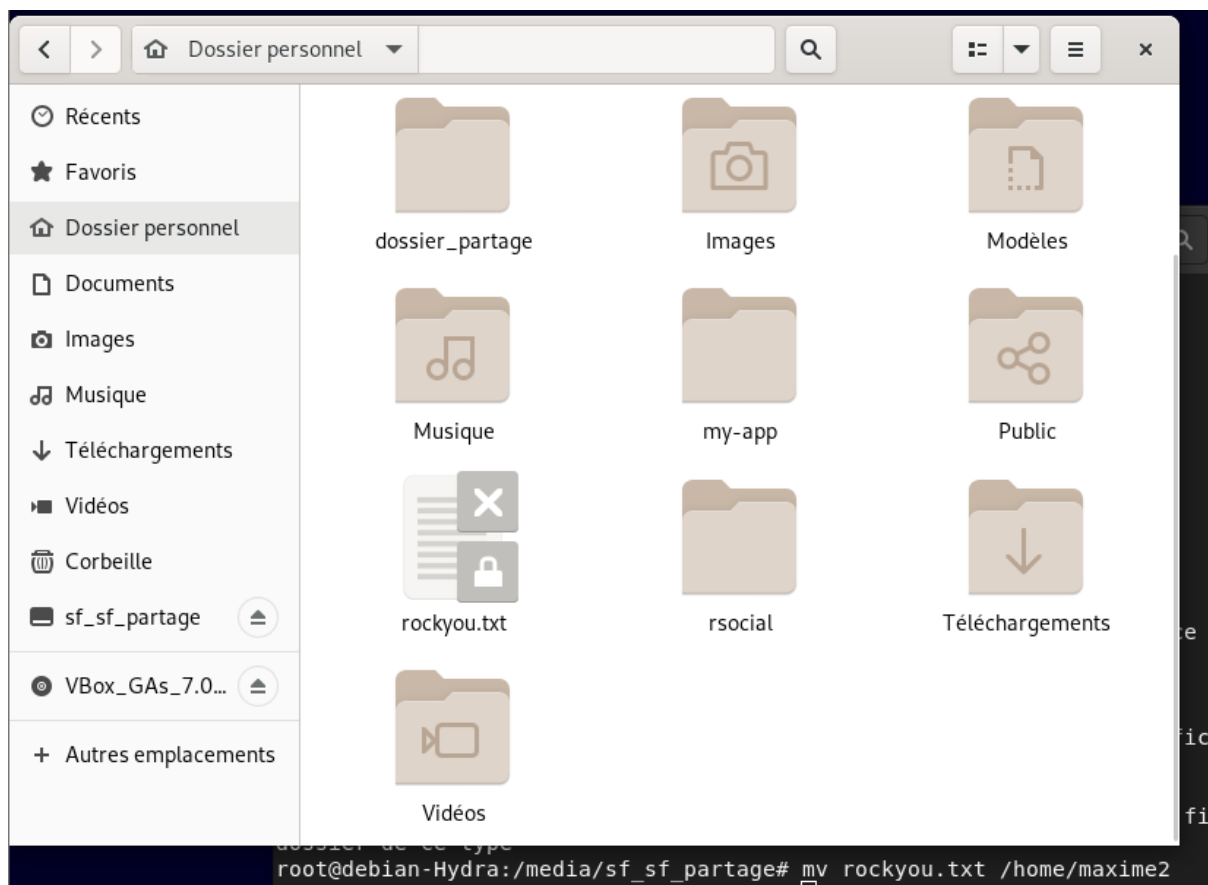
Adresses

Adresse	Masque de réseau	Passerelle
192.168.1.30	255.255.255.0	

DNS

Automatique ☒

Séparer les adresses IP avec des virgules



```
maxime2@debian-Hydra:~$ hydra -l usersssh -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
```

```
maxime2@debian-SSH: ~
Apr 11 16:36:25 debian-SSH polkitd(authority=local): Registered Authentication Agent for
unix-session:2 (system bus name :1.71 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale fr_FR.UTF-8)
Apr 11 16:36:27 debian-SSH gdm-launch-environment]: pam_unix(gdm-launch-environment:session): session closed for user Debian-gdm
Apr 11 16:36:27 debian-SSH polkitd(authority=local): Unregistered Authentication Agent for
unix-session:c1 (system bus name :1.36, object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale fr_FR.UTF-8) (disconnected from bus)
Apr 11 16:36:27 debian-SSH systemd-logind[422]: Session c1 logged out. Waiting for processes to exit.
Apr 11 16:36:27 debian-SSH systemd-logind[422]: Removed session c1.
Apr 11 16:36:28 debian-SSH PackageKit: uid 1002 is trying to obtain org.freedesktop.packagekit.system-sources-refresh auth (only_trusted:0)
Apr 11 16:36:28 debian-SSH PackageKit: uid 1002 obtained auth for org.freedesktop.packagekit.system-sources-refresh
Apr 11 16:36:33 debian-SSH realmd[993]: quitting realmd service after timeout
Apr 11 16:36:33 debian-SSH realmd[993]: stopping service
Apr 11 16:36:49 debian-SSH dbus-daemon[407]: [system] Failed to activate service 'org.bluez': timed out (service start timeout=25000ms)
Apr 11 16:38:30 debian-SSH sudo: maxime2 : TTY=pts/0 ; PWD=/home/maxime2 ; USER=root ; COMMAND=/usr/bin/less /var/log/auth.log
Apr 11 16:38:30 debian-SSH sudo: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1002)
Apr 11 16:41:18 debian-SSH sudo: pam_unix(sudo:session): session closed for user root
Apr 11 16:41:50 debian-SSH sudo: maxime2 : TTY=pts/1 ; PWD=/home/maxime2 ; USER=root ; COMMAND=/usr/bin/less /var/log/auth.log
Apr 11 16:41:50 debian-SSH sudo: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1002)
(END)
```

```
maxime2@debian-Rsyslog: ~
maxime2@debian-Rsyslog:~$ sudo tail -f /var/log/auth.log
[sudo] Mot de passe de maxime2 :
Apr 11 16:43:25 debian-Rsyslog gdm-launch-environment]: pam_systemd(gdm-launch-environment:session): Failed to release session: Appel système interrompu
Apr 11 16:43:25 debian-Rsyslog polkitd(authority=local): Unregistered Authentication Agent for unix-session:c1 (system bus name :1.41, object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale fr_FR.UTF-8) (disconnected from bus)
Apr 11 16:43:25 debian-Rsyslog systemd-logind[436]: Session c1 logged out. Waiting for processes to exit.
Apr 11 16:43:25 debian-Rsyslog systemd-logind[436]: Removed session c1.
Apr 11 16:43:27 debian-Rsyslog PackageKit: uid 1002 is trying to obtain org.freedesktop.packagekit.system-sources-refresh auth (only_trusted:0)
Apr 11 16:43:27 debian-Rsyslog PackageKit: uid 1002 obtained auth for org.freedesktop.packagekit.system-sources-refresh
Apr 11 16:43:36 debian-Rsyslog systemd: pam_unix(systemd-user:session): session closed for user Debian-gdm
Apr 11 16:43:37 debian-Rsyslog dbus-daemon[420]: [system] Failed to activate service 'org.bluez': timed out (service_start timeout=25000ms)
Apr 11 16:43:59 debian-Rsyslog sudo: maxime2 : TTY=pts/0 ; PWD=/home/maxime2 ; USER=root ; COMMAND=/usr/bin/tail -f /var/log/auth.log
Apr 11 16:43:59 debian-Rsyslog sudo: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1002)
```

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.