Université Abdelmalek Essaâdi

Faculté des Sciences et Techniques-Tanger

Département Génie Informatique

Cryptographie-Sécurité Services

TP OpenSSH

Réalisé Par :

Yossra safi chetouan

Installation d'un serveur SSH

```
yossra@debian:~$ apt-cache policy openssh-server
openssh-server:
  Installed: 1:8.4p1-5+deb11u3
  Candidate: 1:8.4p1-5+deb11u3
  Version table:
 *** 1:8.4p1-5+deb11u3 500
        500 http://deb.debian.org/debian bullseye/main amd64 Packages
        500 http://security.debian.org/debian-security bullseye-security/main am
d64 Packages
        100 /var/lib/dpkg/status
yossra@debian:~$
```

```
yossra@debian:~$ ssh -V
OpenSSH_8.4p1 Debian-5+deb11u3, OpenSSL 1.1.1w  11 Sep 2023
yossra@debian:~$
```

Vérifier l'état du service SSH

```
yossra@debian:~$ systemctl status sshd
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: e>
     Active: active (running) since Thu 2024-03-28 20:06:50 EDT; 1min 28s ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 535 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 550 (sshd)
      Tasks: 1 (limit: 2264)
     Memory: 2.1M
        CPU: 76ms
     CGroup: /system.slice/ssh.service
             └─550 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

Warning: some journal files were not opened due to insufficient permissions.
lines 1-14/14 (END)
```
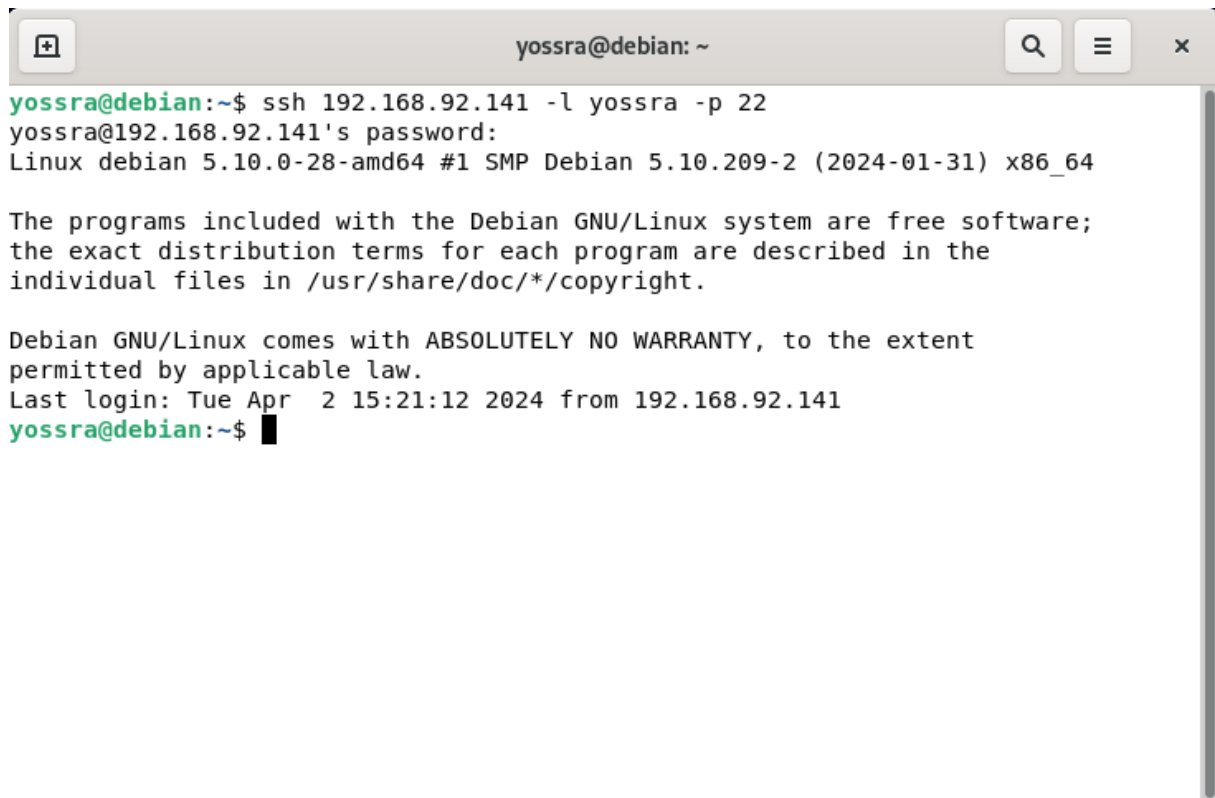
Lister les connexions réseau actives sur un système

```
    Process: 531 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 544 (sshd)
      Tasks: 1 (limit: 2264)
     Memory: 2.3M
        CPU: 596ms
     CGroup: /system.slice/ssh.service
             └─544 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

Warning: some journal files were not opened due to insufficient permissions.

yossra@debian:~$ sudo systemctl start sshd
yossra@debian:~$  ss -lntp |grep ":22
>
> ^C
yossra@debian:~$ su -
Password:
su: Authentication failure
yossra@debian:~$ su -
Password:
root@debian:~# systemctl start sshd
root@debian:~# ss -lntp |grep ":22"
LISTEN 0    128    0.0.0.0:22    0.0.0.0:*    users:(("sshd",pid=544,fd=3))
LISTEN 0    128    [::]:22       [::]:*       users:(("sshd",pid=544,fd=4))
root@debian:~#
```

Connexion client-serveur SSH (192.168.92.141)

```
root@debian:~# hostname -I
192.168.92.141
root@debian:~# █
```

```
yossra@debian:~$ ssh yossra@192.168.92.141
yossra@192.168.92.141's password:
Linux debian 5.10.0-28-amd64 #1 SMP Debian 5.10.209-2 (2024-01-31) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
yossra@debian:~$ █
```

Connexion client-serveur SSH (192.168.92.141)

```
yossra@debian:~$ ssh 192.168.92.141 -l yossra -p 22
yossra@192.168.92.141's password:
Linux debian 5.10.0-28-amd64 #1 SMP Debian 5.10.209-2 (2024-01-31) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Apr  2 15:21:12 2024 from 192.168.92.141
yossra@debian:~$ █
```

OpenSSH : Configuration du serveur SSH

➢ Changer le port d'écoute de 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 7256
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

-- INSERT --                                           15,10          Top
```

```
root@debian:~# vim /etc/ssh/sshd_config
root@debian:~# cat /etc/ssh/sshd_config
#         $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 7256
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key
```

```
root@debian:/etc# cd ..
root@debian:/# cd  /etc/ssh/
root@debian:/etc/ssh# ss -lntp |grep ":7256" |column -t
root@debian:/etc/ssh# service sshd restart
root@debian:/etc/ssh# ss -lntp |grep ":7256"
LISTEN 0      128            0.0.0.0:7256       0.0.0.0:*    users:(("sshd",pid=437
6,fd=3))
LISTEN 0      128            [::]:7256          [::]:*    users:(("sshd",pid=437
6,fd=4))
root@debian:/etc/ssh#
```

➢ Gérer l'IP d'écoute du serveur

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

Port 7256
#AddressFamily any
ListenAddress 192.168.92.141
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
-- INSERT --                                    17,29        10%
```

```
root@debian:/# vim /etc/ssh/sshd_config
root@debian:/# cat /etc/ssh/sshd_config
#         $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 7256
#AddressFamily any
ListenAddress 192.168.92.141
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key
```
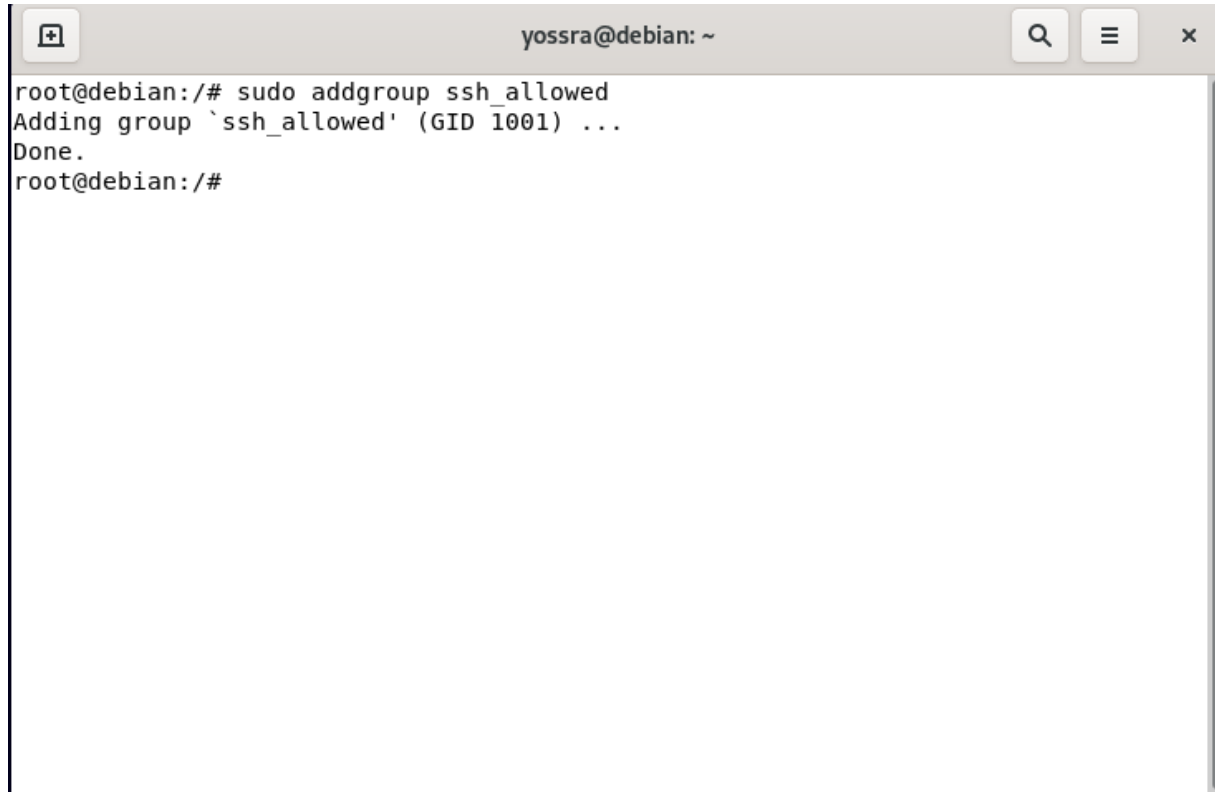
```
root@debian:/# service sshd restart
root@debian:/# ss -lntp |grep ":7256" |column -t
LISTEN  0  128  192.168.92.141:7256  0.0.0.0:*  users:(("sshd",pid=4390,fd=3))
root@debian:/#
```

➢ Ajout des groupes et des utilisateurs :


```
root@debian:/# sudo addgroup ssh_allowed
Adding group `ssh_allowed' (GID 1001) ...
Done.
root@debian:/#
```

```
root@debian:/# sudo adduser u1
Adding user `u1' ...
Adding new group `u1' (1002) ...
Adding new user `u1' (1001) with group `u1' ...
Creating home directory `/home/u1' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
passwd: password unchanged
Try again? [y/N] y
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for u1
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n]
root@debian:/#
```

```
root@debian:/# cd /home
root@debian:/home# ls
u1  yossra
root@debian:/home#
```

```
root@debian:/# sudo usermod -a -G ssh_allowed u1
root@debian:/# cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:yossra
floppy:x:25:yossra
tape:x:26:
sudo:x:27:yossra
audio:x:29:pulse,yossra
```

➢ Gestion des logs


```
Apr  2 18:21:59 debian su: pam_unix(su-l:session): session opened for user root(uid=0) by (ui
d=1000)
Apr  2 18:28:02 debian sshd[544]: Received signal 15; terminating.
Apr  2 18:28:02 debian sshd[4376]: Server listening on 0.0.0.0 port 7256.
Apr  2 18:28:02 debian sshd[4376]: Server listening on :: port 7256.
Apr  2 18:30:01 debian CRON[4380]: pam_unix(cron:session): session opened for user root(uid=0
) by (uid=0)
Apr  2 18:30:01 debian CRON[4380]: pam_unix(cron:session): session closed for user root
Apr  2 18:32:14 debian sshd[4376]: Received signal 15; terminating.
Apr  2 18:32:15 debian sshd[4390]: Server listening on 192.168.92.141 port 7256.
Apr  2 18:36:44 debian sudo:     root : TTY=pts/0 ; PWD=/ ; USER=root ; COMMAND=/usr/sbin/add
group ssh_allowed
Apr  2 18:36:44 debian sudo: pam_unix(sudo:session): session opened for user root(uid=0) by (
uid=0)
Apr  2 18:36:44 debian groupadd[4403]: group added to /etc/group: name=ssh_allowed, GID=1001
Apr  2 18:36:44 debian groupadd[4403]: group added to /etc/gshadow: name=ssh_allowed
Apr  2 18:36:44 debian groupadd[4403]: new group: name=ssh_allowed, GID=1001
Apr  2 18:36:44 debian sudo: pam_unix(sudo:session): session closed for user root
Apr  2 18:37:33 debian sudo:     root : TTY=pts/0 ; PWD=/ ; USER=root ; COMMAND=/usr/sbin/add
group ssh_allowed
Apr  2 18:37:33 debian sudo: pam_unix(sudo:session): session opened for user root(uid=0) by (
uid=0)
Apr  2 18:37:33 debian sudo: pam_unix(sudo:session): session closed for user root
                                                              432,1              91%
```

➢ Bannière de connexion SSH


```
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"/etc/motd" 7L, 286B                                      1,0-1        All
```



```
========================================================
connexion etablie avec succes.
Merci de respecter la politique de securite.
Tous acces par une perssone non habilite est interdit.
========================================================
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
-- INSERT --                                            1,59         All
```

```
root@debian:/# sudo vim /etc/motd
root@debian:/# cat /etc/motd
========================================================
connexion etablie avec succes.
Merci de respecter la politique de securite.
Tous acces par une perssone non habilite est interdit.
========================================================
root@debian:/# █
```
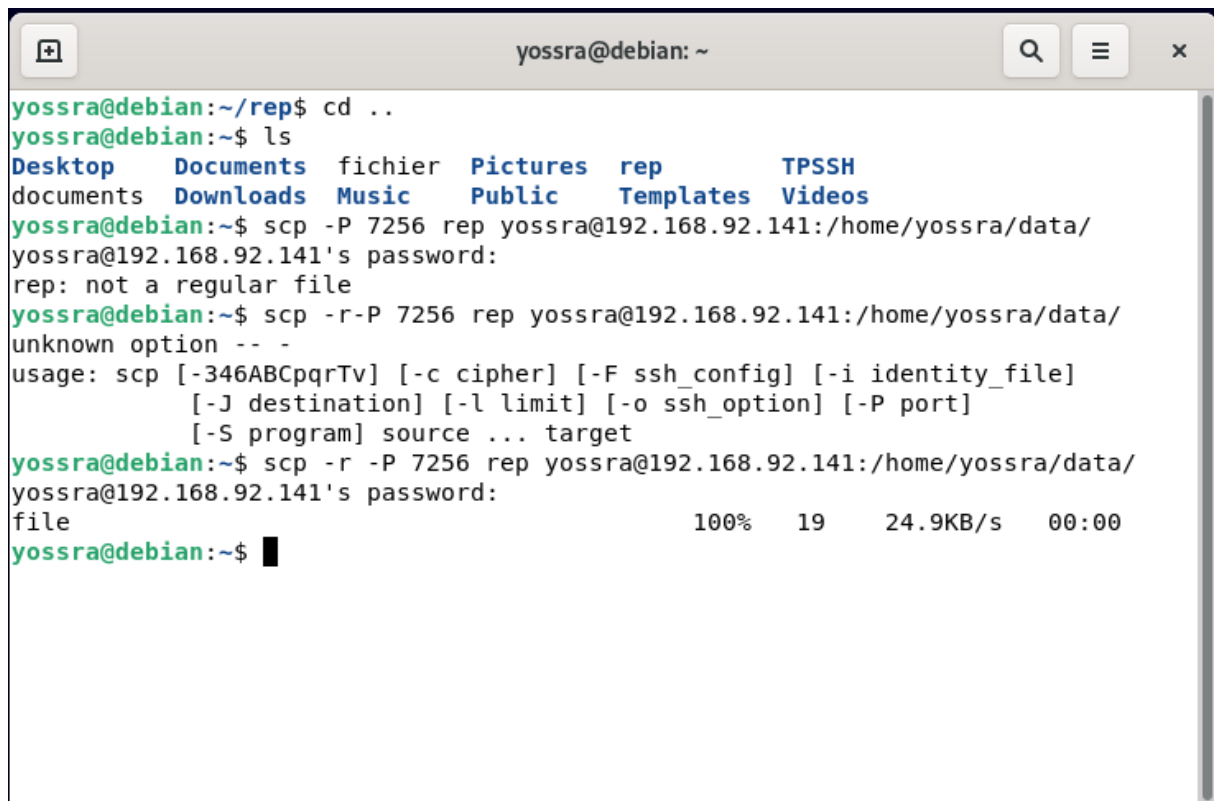
Transfert de fichier via SSH

➤ SCP : Secure Copy

- Copie d'un fichier depuis le répertoire courant vers un répertoire du serveur:


```
yossra@debian:~$ ls
Desktop     Downloads  Music     Public      TPSSH
Documents   fichier    Pictures  Templates   Videos
yossra@debian:~$ scp -P 7256 fichier yossra@192.168.92.141:/home/yossra/document
s
yossra@192.168.92.141's password:
fichier                                      100%   46    32.4KB/s   00:00
yossra@debian:~$ █
```

- Copie d'un répertoire, avec éventuellement ses sous-répertoires, vers un répertoire du serveur

```
yossra@debian:~/rep$ cd ..
yossra@debian:~$ ls
Desktop    Documents  fichier  Pictures  rep       TPSSH
documents  Downloads  Music    Public    Templates  Videos
yossra@debian:~$ scp -P 7256 rep yossra@192.168.92.141:/home/yossra/data/
yossra@192.168.92.141's password:
rep: not a regular file
yossra@debian:~$ scp -r-P 7256 rep yossra@192.168.92.141:/home/yossra/data/
unknown option -- -
usage: scp [-346ABCpqrTv] [-c cipher] [-F ssh_config] [-i identity_file]
           [-J destination] [-l limit] [-o ssh_option] [-P port]
           [-S program] source ... target
yossra@debian:~$ scp -r -P 7256 rep yossra@192.168.92.141:/home/yossra/data/
yossra@192.168.92.141's password:
file                                          100%   19    24.9KB/s   00:00
yossra@debian:~$ ▌
```
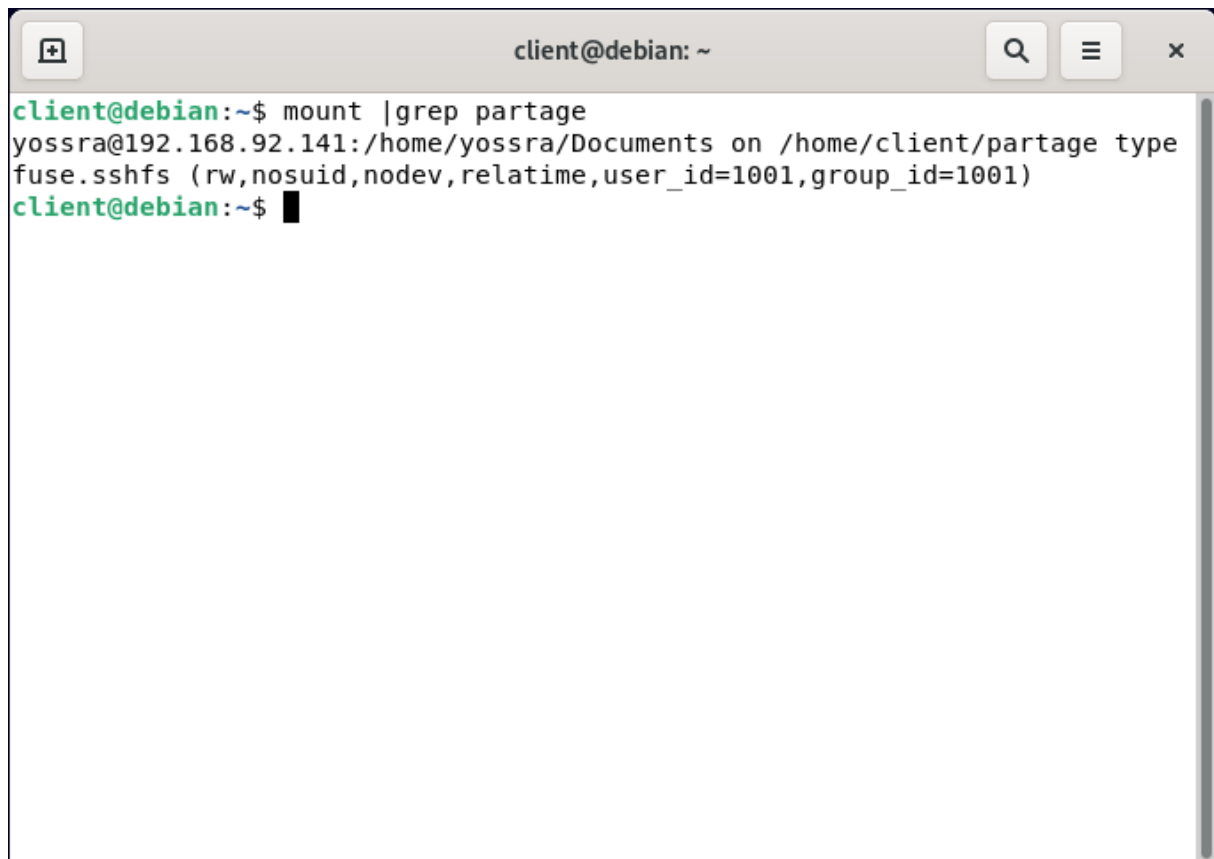
➢ SFTP : Secure FTP

```
# 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


~
~
~
~
~
~
                                              114,0-1      Bot
```

```
client@debian:/$ mkdir /home/client/partage
client@debian:/$
```

```
root@debian:/# su client
client@debian:/$ apt-get install sshfs
E: Could not open lock file /var/lib/dpkg/lock-frontend - open (13: Permission d
enied)
E: Unable to acquire the dpkg frontend lock (/var/lib/dpkg/lock-frontend), are y
ou root?
client@debian:/$ sudo apt-get install sshfs
[sudo] password for client:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  sshfs
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 46.0 kB of archives.
After this operation, 125 kB of additional disk space will be used.
Get:1 http://deb.debian.org/debian bullseye/main amd64 sshfs amd64 3.7.1+repack-
2 [46.0 kB]
Fetched 46.0 kB in 1s (42.8 kB/s)
Selecting previously unselected package sshfs.
(Reading database ... 141463 files and directories currently installed.)
Preparing to unpack .../sshfs_3.7.1+repack-2_amd64.deb ...
Unpacking sshfs (3.7.1+repack-2) ...
Setting up sshfs (3.7.1+repack-2) ...
Processing triggers for man-db (2.9.4-2) ...
client@debian:/$
```

```
client@debian:~$ sshfs -p 7256 yossra@192.168.92.141:/home/yossra/Documents /hom
e/client/partage
yossra@192.168.92.141's password:
client@debian:~$
```

```
client@debian:~$ mount |grep partage
yossra@192.168.92.141:/home/yossra/Documents on /home/client/partage type
fuse.sshfs (rw,nosuid,nodev,relatime,user_id=1001,group_id=1001)
client@debian:~$
```
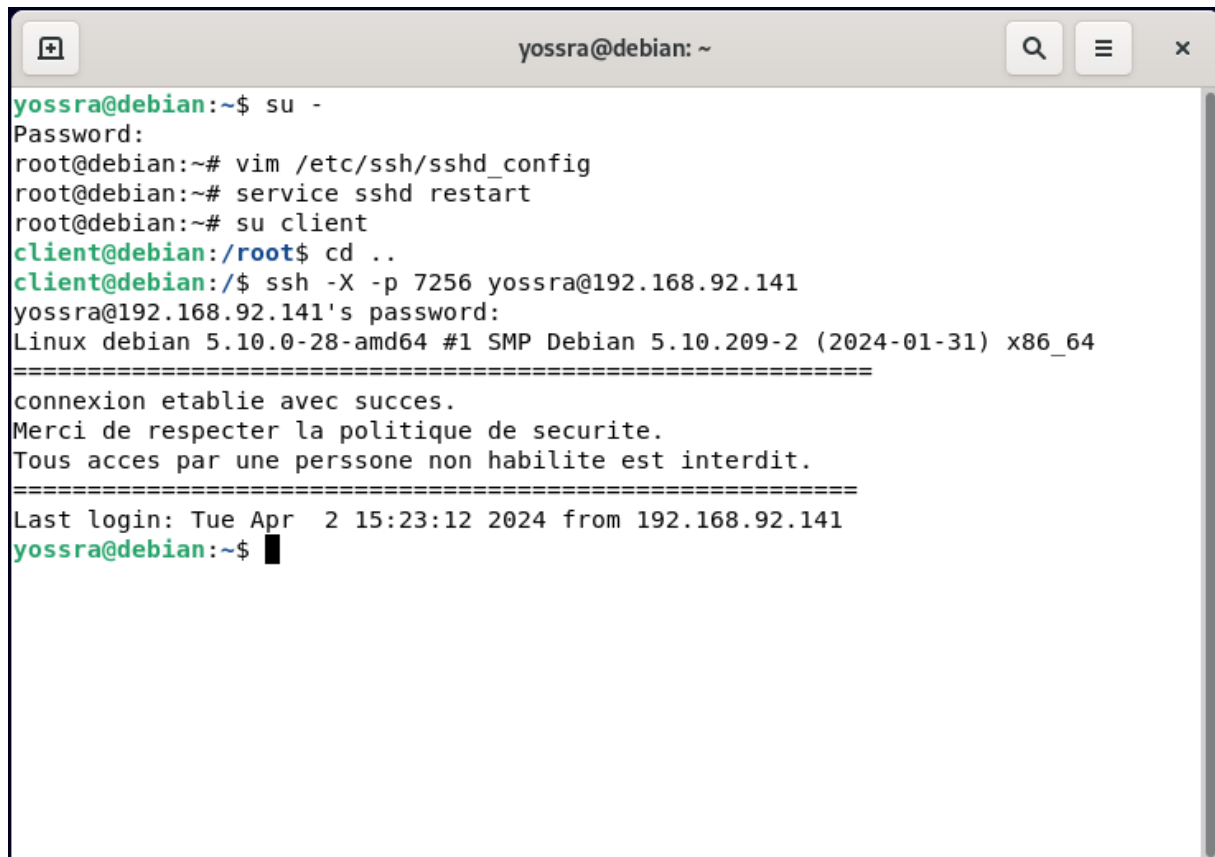
> SSH : X11 Forwarding
- Configuration X11 Forwarding coté serveur

```
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and ChallengeResponseAuthentication to 'no'.
UsePAM yes

#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
PrintMotd no
#PrintLastLog yes
#TCPKeepAlive yes
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#UseDNS no
#PidFile /var/run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
-- INSERT --                                          100,23          81%
```
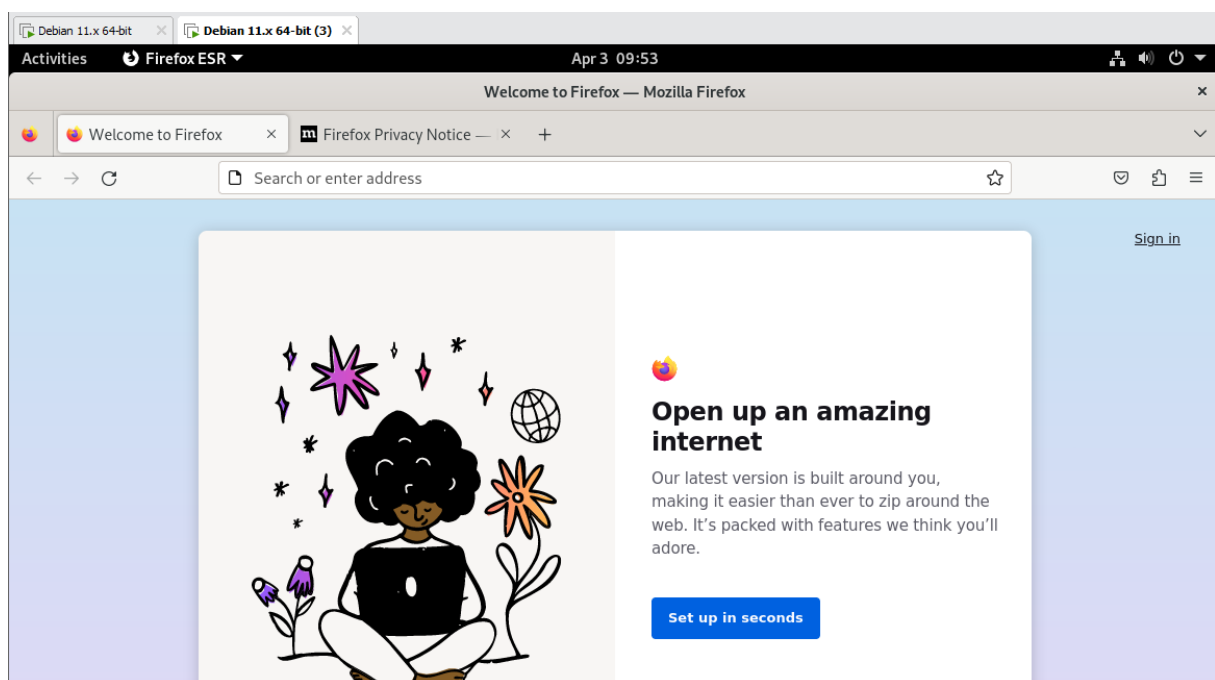
```
yossra@debian:~$ su -
Password:
root@debian:~# vim /etc/ssh/sshd_config
root@debian:~# service sshd restart
root@debian:~#
```

- Établir la connexion SSH (Secure Shell) avec serveur

```
yossra@debian:~$ su -
Password:
root@debian:~# vim /etc/ssh/sshd_config
root@debian:~# service sshd restart
root@debian:~# su client
client@debian:/root$ cd ..
client@debian:/$ ssh -X -p 7256 yossra@192.168.92.141
yossra@192.168.92.141's password:
Linux debian 5.10.0-28-amd64 #1 SMP Debian 5.10.209-2 (2024-01-31) x86_64
=========================================================
connexion etablie avec succes.
Merci de respecter la politique de securite.
Tous acces par une perssone non habilite est interdit.
=========================================================
Last login: Tue Apr  2 15:23:12 2024 from 192.168.92.141
yossra@debian:~$ 
```

- Lancer le navigateur web Firefox

Authentification SSH par clés

➢ Génération de la clé

```
client@debian: ~

client@debian:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/client/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/client/.ssh/id_rsa
Your public key has been saved in /home/client/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:S75B4CIrkXWd5ym8skRDg18YLkjqbY96nu9FjGTFxDk client@debian
The key's randomart image is:
+---[RSA 3072]----+
| .   . +o.       |
|o. o +.E         |
|o + *o= o        |
|.o.=o=o+ .       |
|o..o=.+oS        |
| ..+oo.* .       |
|. ..o...+        |
| ..o.o.  o       |
| .oo+o   .       |
+----[SHA256]-----+
client@debian:~$ █
```

```
client@debian:~$ cd /home/client/.ssh/
client@debian:~/.ssh$ ls
id_rsa  id_rsa.pub  known_hosts
client@debian:~/.ssh$ cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABDVJkgiTL
FwcQspWm4pPmq8AAAAEAAAAAEAAAGXAAAAB3NzaC1yc2EAAAADAQABAAABgQCwxPEwf88Z
CGXoB2KNSWq4aQSt9BLPHStEKKiP2rN9mU/qKYu1IArC4HXWabmFcRfwXtjHYj9FRX9l+i
+iRYNmhOVeFpjzHkRYaxbctm5BfLUxD/bmZ2YLL9ZksAovxowyHcttEpCKfYYCRwMhfASf
FSnmyt0zkUnH5I9p+XCxv7oIeWVWVUjYgjsUvcaKArGFfLsNZH7wQarmqEq513/psTgxJ7
G3h7ReO8tzipLSk3Ur3Val6+YL46blYRWr5gcxI9D4vEvC5uES9ggtnCDDp+fPoz6l1x49
RgJB61oMBsRgD/VyLqJxi9srSSmyRQZcXX5jR00j5zmCIBbh9KHD4RTNq+FtuxJ/QX9XZz
WOgME6MbHbB/0CirPIDUkjAhYtegengy7YpC4h1TPI1RO2W5j16N/qr5psl8i2vATKkfa2
ODB3Sk9j2Eg5Aa1qopKp/ZNW4iPBs2Gz+9x/WVuQEEILHOdt1fftq1qlkrTlaue86qIJr7
dULPexgABGwMEAAAWQxeQZny3zbdKNHUycsIY/BPrzTiK0ARswqJnETglCmmIV9rhg+/y+
0pobKOTlwcKuOZXeNsXDSANrfugUQOiq35ZOgiN9YTt5WaWboUQVlprPUSl6NJjeJIuj1c
FmQllDNbgHSGrm6GCoqXrhfDeHtWK4hKAKFrhN/eutq+k56IgMl+jS2srbm0LOTAF15O+R
O2F/yQpJhYDA7l9RJaffY7oWWjtvFabeP8KU1JYOK4267ue6ONOTTeDSCHrTi1oweS2Xsv
9aCQ40EKEnWgpKzdWSGTiJuuwLxN+ux/Nix6d+1IxexolgHK22w9C8kBO6rfrFUiEvK6GF
3Yfc2Jf/Lhp4ta8reclfT1QMepa2dw4PA2raScq7/qcO+gDPfA6Wghi7/xjynKVFaD/L94
ihTq4iUcJ04NLCL38ZrjRJwugfMxGDZNHSzqtoh6HOPO6rfnfBYrwRWVHpO8OB/jKqekxZ
HqNbXn2gtmV1FkRiV/WgFGw4XAgKCUZtkGe9cdx9rIdENTKGjlw1CekGUz4RXyZHlLH9a9
o1hlXDbAZJ0sRS1Z4wChh2umTMww2F0vTJOCRgvtOuzzJZonOnhMPp1WLhLvxlSizErUg8
nAkczTfdLaoT2ZgYkvikP5JCYggHCV1P5lfz1hmvcw6S85Wv3IIdP3OFCgwKNxNeSSBxRO
5gSUTtL7J2CmjTrLClCMKjeSLm9mmEbg0ws8x4DJWOPT/MaVX9YcCvqSThbCLsJVu3E19a
CsHdd1KtgHBrv7N0dRVLrB+31RxOyIfgyCE7PU3cgPkaqku43fH5b7jdbTtSLJ9GGy/Irr
```

```
client@debian:~$ ls -al .ssh
total 20
drwx------   2 client client 4096 Apr  3 10:02 .
drwxr-xr-x 16 client client 4096 Apr  3 09:26 ..
-rw-------   1 client client 2655 Apr  3 10:04 id_rsa
-rw-r--r--   1 client client  567 Apr  3 10:04 id_rsa.pub
-rw-r--r--   1 client client  222 Apr  2 20:25 known_hosts
client@debian:~$ 
```

➢ Mettre la clé sur le serveur


```
client@debian:~$ ssh-copy-id -i ~/.ssh/id_rsa.pub -p 7256 yossra@192.168.92.141
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/client/.ssh
/id_rsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter
out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompt
ed now it is to install the new keys
yossra@192.168.92.141's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh -p '7256' 'yossra@192.168.92.141'
"
and check to make sure that only the key(s) you wanted were added.

client@debian:~$
```