TP - Admin à distance

que vous donne cette commande

la commande donne le chemin a vers SSH utilisé par notre système

```
root@samba:/home/vboxuser# which ssh
/usr/bin/ssh
```

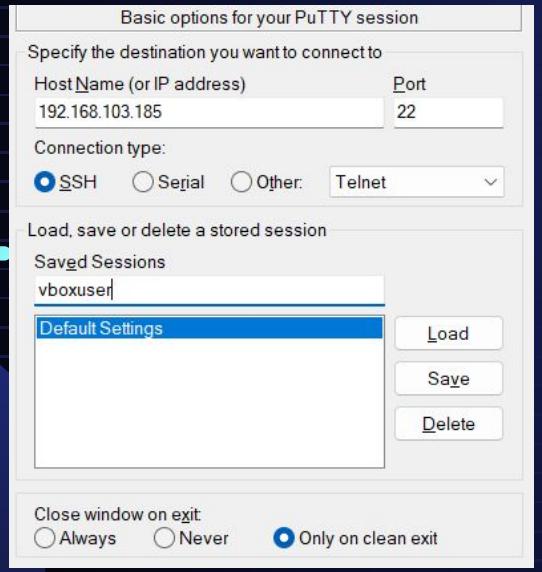
installer ssh

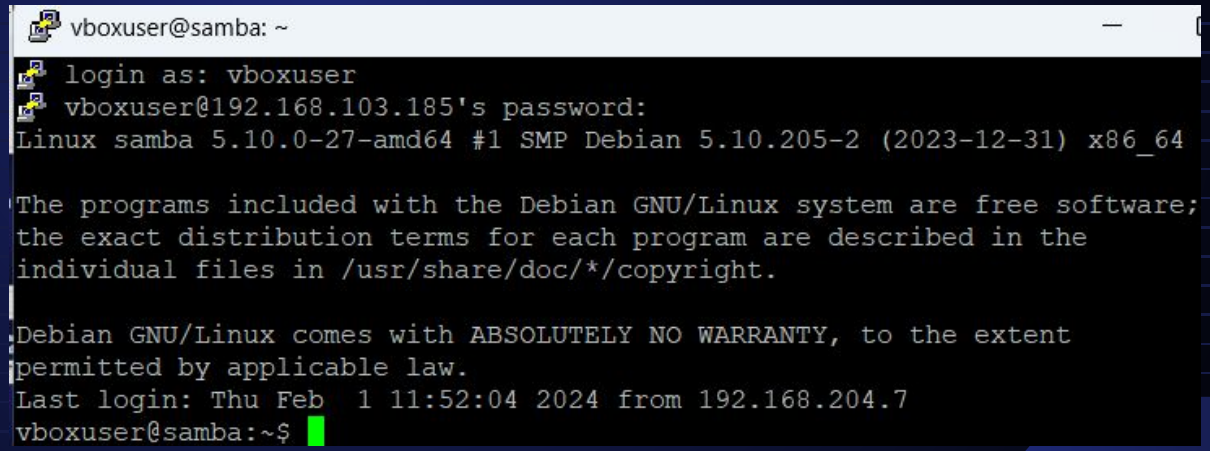
Tout simplement faire apt install openssh-server pour instaler ssh

```
root@samba:/home/vboxuser# apt install openssh-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
openssh-server is already the newest version (1:8.4p1-5+deb11u3).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@samba:/home/vboxuser#
```

Configuration simple d'une connexion ssh sous windows avec putty

Nous mettons l'ip du serveur ssh et le port 22 et on arrive sur le login donc ici on peut mettre le nom de la vm ou root et le mdp de la vm



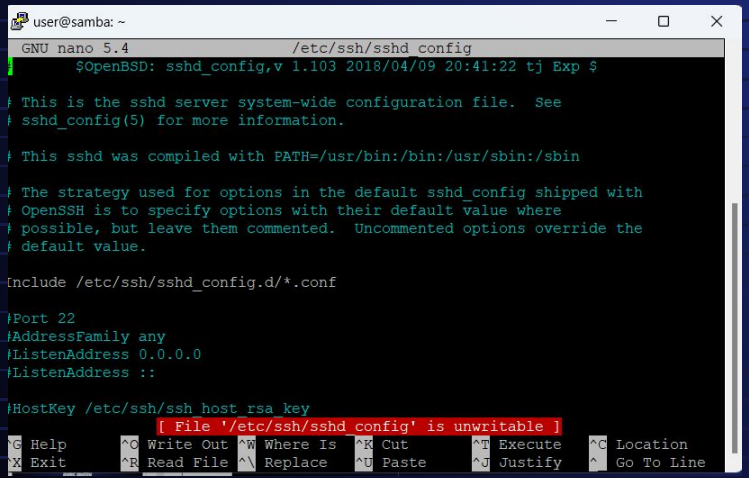


user

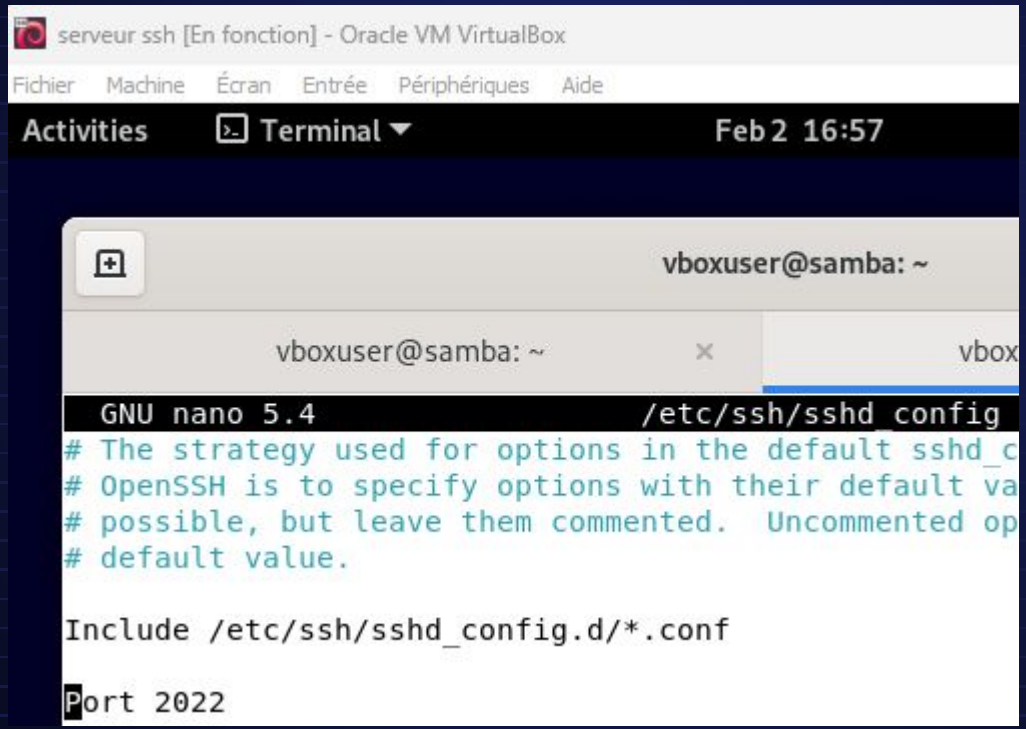
Le user arrive dans le répertoire /home/user

```
user@samba:~$ pwd
/home/user
```

il ne peut pas modifier car il n'est pas admis dans la base de données des admin

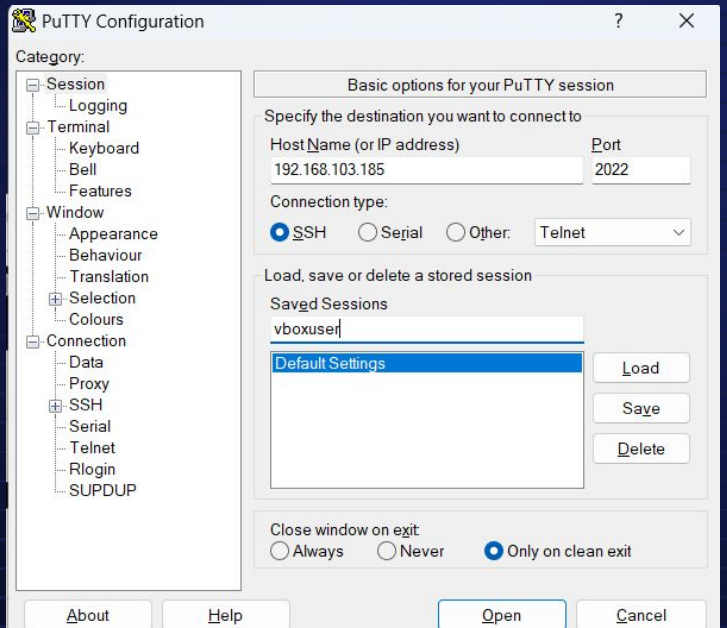


changer le port



Retentez une connexion au serveur. Que se passe-t-il

Si on met port 2022 dans putty cela va fonctionner cependant si on laisse le port en 22 sur putty ça ne fonctionnera pas

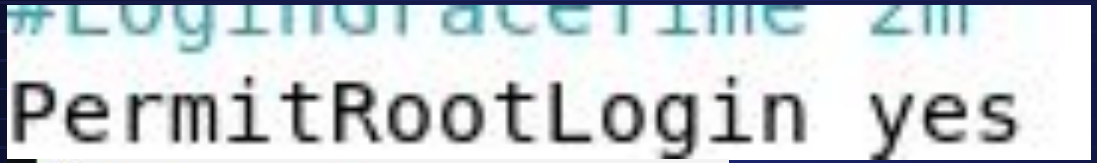


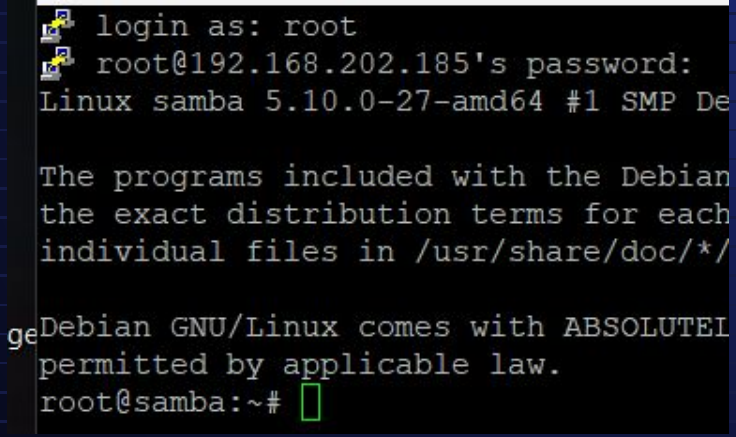
Que faut-il faire pour établir une connexion au serveur? Quel est l'intérêt d'un changement de port ?

L'intérêt de changer le port d'écoute SSH est d'ajouter une couche supplémentaire de sécurité en rendant plus difficile la découverte du port d'écoute.

Autorisation login root dans le nano

on ouvre le nano /etc/ssh/sshd_config et on met cette commande pour autoriser une connexion au serveur avec le login root



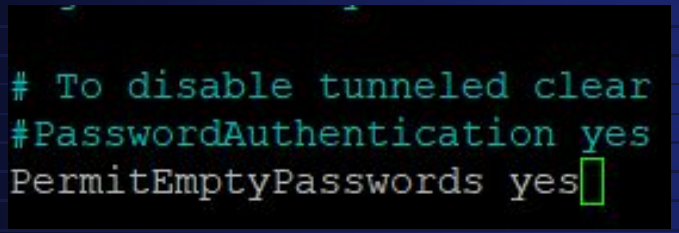


Pourquoi est-ce que la permission donnée (ou pas) à root est-elle importante à maîtriser

Car si donne l'accès à root au serveur on pourra se connecter au serveur ou pas

Permettre les mots de passe vide

Si on met sur yes cette option cela va nous demander un identifiant et mdp or elle est mise sur no de base ce qui est pas très sécurisé de base



Quelle est la différence entre PermitEmptyPasswords no et PermitRootLogin without-password ?

PermitEmptyPasswords no interdit les connexions avec des mots de passe vides pour tous les utilisateurs, tandis que PermitRootLogin without-password permet à l'utilisateur root de se connecter uniquement avec des clés SSH, pas avec un mot de passe.

Ajouter les user dans les groupes

Après avoir créé les user avec la commande adduser on les ajoute avec la commande usermod dans les groupes

```
usermod -aG etudiant user1
usermod -aG ssh user1
usermod -aG ssh user2
usermod -aG etudiant user3
```

Changer les mdp des user

Pour pouvoir les changer il faut être en superuser , pour ce faire il faut effectuer la commande sudo -i et entrer chpasswd et mettre user:mdp

```
root@samba:~# chpasswd
user1:Password1
user2:Password1
user3:Password1
root@samba:~#
```

Gérer l'échange des clés publiques

On creer un répertoire nommé ssh pour chaque utilisateur et un répertoire ssh pour le user root

```
root@samba:~# mkdir /home/user1/.ssh
root@samba:~# mkdir /home/user2/.ssh
root@samba:~# mkdir /home/user3/.ssh
root@samba:~# mkdir /home
mkdir: cannot create directory '/home': File exists
root@samba:~# mkdir /home/.ssh
root@samba:~#
```

Gérer l'échange des clés publiques

Et sur chacun de ces répertoires, on change les droits :

```
root@samba:~# cd /home/user1
root@samba:/home/user1# chmod0770 .ssh
-bash: chmod0770: command not found
root@samba:/home/user1# chmod 0770 .ssh
root@samba:/home/user1# cd ..
root@samba:/home# cd /home/user2
root@samba:/home/user2# chmod 0770 .ssh
root@samba:/home/user2# cd /home/user2
root@samba:/home/user2# cd /home/user3
root@samba:/home/user3# chmod 0770 .ssh
root@samba:/home/user3# cd ..
root@samba:/home# chmod 0770 .ssh
root@samba:/home#
```

Gérer l'échange des clés publiques

Sur le user1 et autre user on va créer une clé DSA. La commande ci dessous va générer une clé publique et privé et on mettra un mdp sio2018

```
root@vierge:~# ssh-keygen -t dsa -f  ~/.ssh/id_dsa
Generating public/private dsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_dsa
Your public key has been saved in /root/.ssh/id_dsa.pub
The key fingerprint is:
SHA256:uVP3GBygZ2hiaUTZ5tSRHHf5C+CZL8OdJCn+1WmBaJQ root@vierge
The key's randomart image is:
+---[DSA 1024]----+
|      .oo o++o .. |
|     ...+o+E ..   |
|      =++ = B .. |
|     o o.= X = ..|
|        S = O + +|
|         + = O = |
|        o . = o  |
|         . .     |
|                 |
```

Gérer l'échange des clés publiques

On va afficher la clé publique et privé avec la commande ci dessous

```
root@vierge:~# cat ~/.ssh/id_dsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABCkadCIM4
wS6cR0JbQonLS6AAAAEAAAAAEAAAGxAAAAB3NzaC1kc3MAAACBAIJmLjxxZ2mdNU7If2Fm
LsA0I3O4SK4+Lm4g4bquRR02P47vuT9yF3Mvg74KkrtqPbsk1oLnI0gpqgTfQWX/MdXy/t
S4eO+HrnIuPw4KFfXDrjc3adB/C2Q2PVxq//02h3y9z44+72uRFIryVlNeehYzNuHHbjlX
KbZxY4feykDDAAAAFQDwt7bKHWL2g5c19CjBT3YcVzQEmQAAAIAyxx4Cws3ReDmFaT0qUL
v+zO8N9+Ihzt5b3DMMAraU+YWFRXkSlhqm2vOF1ctEtFGT1Y7nraVC8Gi2xT9vZnGN3Y1o
XdOFHhhJnIUi7zJXRFsbtMuJuBQJJYqCQcQ3eOlvliRqzX3EAHN7b2U7jZlfCAv46cdB4C
DOrjl4A2CMzAAAAIBQlfgawggy7nfBmSyHeJVHoeF15iMWwgOGeppXQ9VJbMz+WbA4V7XU
lqMoLxHp3H7Fh55tU6Yqqc1JyKrgnRrG2/nUG6AUBLf3mAB+zu0PFPMXzND0/25WfNyoG4
22TBCs+NWtOX0oXGCZOxDcwR5I95GLscuvZ0fPw6QOFS06CQAAAeDx5ZyJ1hN93nwj8Syw
Z0jceRplc/94cp/vDcGdQFcUkSHUbFdrG+6AIaFecRpAnnd7juwlzIXbnnBlX94xuWqMso
tYsa6DmV2vWKyKNlK8KGKMmJQy6MwU9tn3stWXIUtJQYBLG7e9P/kJlY0VsdbM8GMt8KDQ
oB+836nXsIOq5MWzp84Xfqs01nWEtNqRXWltzaESb5xMK2M37JZy9TmOjYHAlHCuIeEWjE
I5NKhUwOvIHjklaMbcDZ06RrR4yBZOBSlvNKzqpS0HnlnZBf0BCugvyM42z/mBTEvt/UL8
zmZkZPul0wnHSCL4iGxldovpULs8vj4g2m5rgpMkySasT4069PhKwo3CI/EfAfbV74JEG5
7dcBdaobpVYdjypLPZI7J2PbfaQg0wrVKDpxc6N5e2T6r3EqTbWIlKVYxU1JxMW61Eohaa
AvPoSfi/TM5W34V1JLXPSjdAUSuuATaDgrqgh/7T5J9VAuYZcznLbptNEOiXGKTKNyayef
PQl+YsIGIR8ldxdP43TkFv9YVCeky8T23Pi9VcR8N4+fqd8W2ltfKV3SVYkdM7Aes0u1ZB
iqfnN2FiIVPqMrp4KLO+oGNfAV0cf4Q+Q14ZWdoWJrjwzSDnoPkWfEm1iFZGcwY=
-----END OPENSSH PRIVATE KEY-----
```

```
root@vierge:~# cat ~/.ssh/id_dsa.pub
ssh-dss AAAAB3NzaC1kc3MAAACBAIJmLjxxZ2mdNU7If2FmLsA0I3O4SK4+Lm4g4bquRR02P47vuT9y
F3Mvg74KkrtqPbsk1oLnI0gpqgTfQWX/MdXy/tS4eO+HrnIuPw4KFfXDrjc3adB/C2Q2PVxq//02h3y9
z44+72uRFIryVlNeehYzNuHHbjlXKbZxY4feykDDAAAAFQDwt7bKHWL2g5c19CjBT3YcVzQEmQAAAIAy
xx4Cws3ReDmFaT0qULv+zO8N9+Ihzt5b3DMMAraU+YWFRXkSlhqm2vOF1ctEtFGT1Y7nraVC8Gi2xT9v
ZnGN3Y1oXdOFHhhJnIUi7zJXRFsbtMuJuBQJJYqCQcQ3eOlvliRqzX3EAHN7b2U7jZlfCAv46cdB4CDO
rjl4A2CMzAAAAIBQlfgawggy7nfBmSyHeJVHoeF15iMWwgOGeppXQ9VJbMz+WbA4V7XU1qMoLxHp3H7F
h55tU6Yqqc1JyKrgnRrG2/nUG6AUBLf3mAB+zu0PFPMXzND0/25WfNyoG422TBCs+NWtOX0oXGCZOxDc
wR5I95GLscuvZ0fPw6QOFS06CQ== root@vierge
```

Deux fichiers sont générés. Affichez les deux. Y-a-t-il une différence? Est-ce normal et pourquoi

Ensuite, il faut envoyer une clé publique au serveur pour qu'il puisse nous identifier

On utilise la commande ci dessous en mettant bien l'ip du serveur

```
root@vierge:~# ssh-copy-id -i ~/.ssh/id_dsa.pub root@192.168.103.185
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_dsa.pu
b"
The authenticity of host '192.168.103.185 (192.168.103.185)' can't be established.
ECDSA key fingerprint is SHA256:nsfoLr90Vjry+iv8BZ7bPafg1/5dCwfCY6F34N1JJ/8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/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 prompted
now it is to install the new keys
root@192.168.103.185's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'root@192.168.103.185'"
and check to make sure that only the key(s) you wanted were added.

root@vierge:~#
```

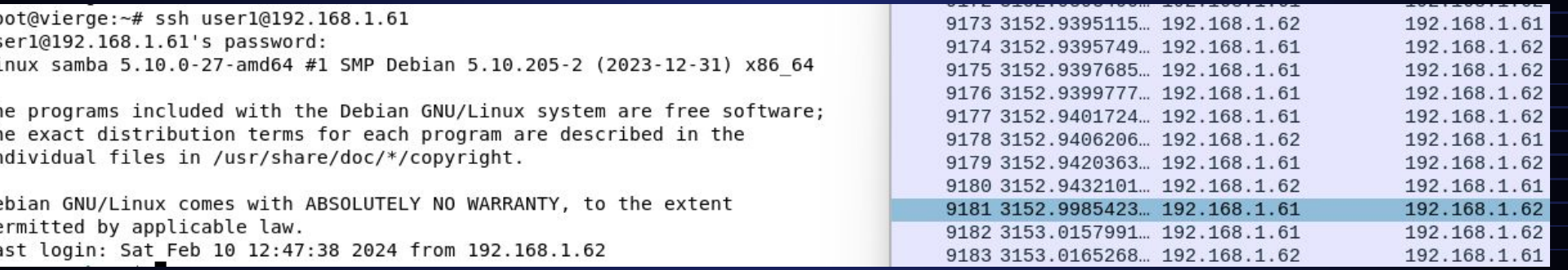
Gérer l'échange des clés publiques

en faisant la commande ~/.ssh/authorized_keys qui fait référence au fichier sur le système Linux qui stocke les clés publiques autorisée on y trouve deux clé publique autorisés

```
root@samba:~/.ssh# cat ~/.ssh/authorized_keys
ssh-dss AAAAB3NzaC1kc3MAAACBAK8/SbhpiZbKg5vvwHXyDhJXaAOV5+jsxrh1bUdeVXJh05vvHj6t
52miG4SlVFWVdjrjsh0pS6I9kz6ZT3BcITxbWwfHWm/v4cNdXQq9KBA4V1TMwq2x8VJFeeAsVt6XEG1f
q6bnnVSerSroBcKxDVNpM1XDmShbaUeOOQZoGauDAAAAFQD1U4eEH2FX3cludXVPuHcFZQvcHwAAAIEA
j7N9gO+ZsgreSFpFX/paI6U0Z+bFkSMGC4Bho/YB2oCO5PVnNT824Kg8OijnIYtUPhoKV6IxMi69FrIO
XIQY8CgKqcSNwsKjzV0KbulUmFL+pinVzcYRKVNxPgPAdfve7KhJdNL/VSipPedkNXT04X0o2JBeBvXO
f5iqLH3+WkYAAACAK5i+9KV3oSNlfxOkF1YxVh+TVJ0fqQR+HbUoLaloPnxiUYv6LsG7l2hLxHn8PWZW
BGMdOCaMxNCfFbYkFnQnLNrrAxd2UjxWTLxjR+Pr3n8k2zXjs5Z8yH6wL5/IqttH3BLLAbiC5J3C81U2
e+0pbw8U7oJwdREtysOaWAtr16Y= root@samba
ssh-dss AAAAB3NzaC1kc3MAAACBAMoFwdJMkRT/noay8YoJK9FVq2rbLN3GPo/46Q+qCrpparoZ8eEe
1Gg84hFmKa/rWHvlyEazoDqZkVxI0K1koDjuOospCYANybRHcl3FYTvmhjVTtC7Ec/naRxL9QWc3UHmQ
rIiDKVQJQdC2woFhNf55Su727ZeqmZjHMpUH9QbnAAAAFQDpZfVYkKOHHUkKy+RJS6ZlWdjuvwAAAIEA
gP6Qa8DOgtiW+1tTDs9LYjiscewl/7EfuABbUlITKe5mplfCKnE5PayfPj06cISyUJShA8cTOfWbH1w0
jW2+gMh0yGj9TYcMWY43APSCVAO0u2s8R01IdHKJB+VHqrCojXD4tegxesMjQ/Yo/FdKaPjA6A2UxIPS
S+16FjBJ040AAACAB/Ne7RgC4xARvJzKvOWT9Q99Whfll+rLSkNTLlcsDz4F5jujb1KS2QQvqXhs+Yr5
CASGxxBUtOgkAr1QIAwDRbYzpe/8V2ADG/itgO7tl6uHL1eIExsQaX0H+fjNszvXUXIUPEdD/I0EfCeX
```

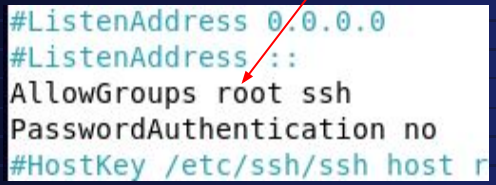
Tester la connexion

Avec la commande ssh user@ipserveurssh et mdp qu'on a créé pour celui ci on peut se connecter et voir une trame sur wireshark



Dans le fichier de configuration du serveur

Si on veut que seulement les user dans certain groupe accède au serveur on fait la commande ci dessous



On peut voir que user3 ne peut pas accéder car il est dans le groupe étudient

(rappel de qui on à ajouté)

```
usermod -aG etudiant user1
usermod -aG ssh user1
usermod -aG ssh user2
usermod -aG etudiant user3
```

```
Permission denied, please try again.
user3@192.168.103.185's password:

root@vierge:/home/vboxuser# ssh user2@192.168.103.185
user2@192.168.103.185's password:
Linux samba 5.10.0-27-amd64 #1 SMP Debian 5.10.205-2 (2023-12-31) 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: Fri Feb  9 15:07:03 2024 from 192.168.103.173
user2@samba:~$ ^C
user2@samba:~$
```

Seul le user3 ne devrait pas pouvoir accéder au serveur ssh mais tout les autres oui

```
root@vierge:/home/vboxuser# ssh root@192.168.103.185
root@192.168.103.185's password:
Linux samba 5.10.0-27-amd64 #1 SMP Debian 5.10.205-2 (2023-12-31) 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: Fri Feb  9 14:02:47 2024 from 192.168.103.173
root@samba:~# ^C
root@samba:~# exit
```