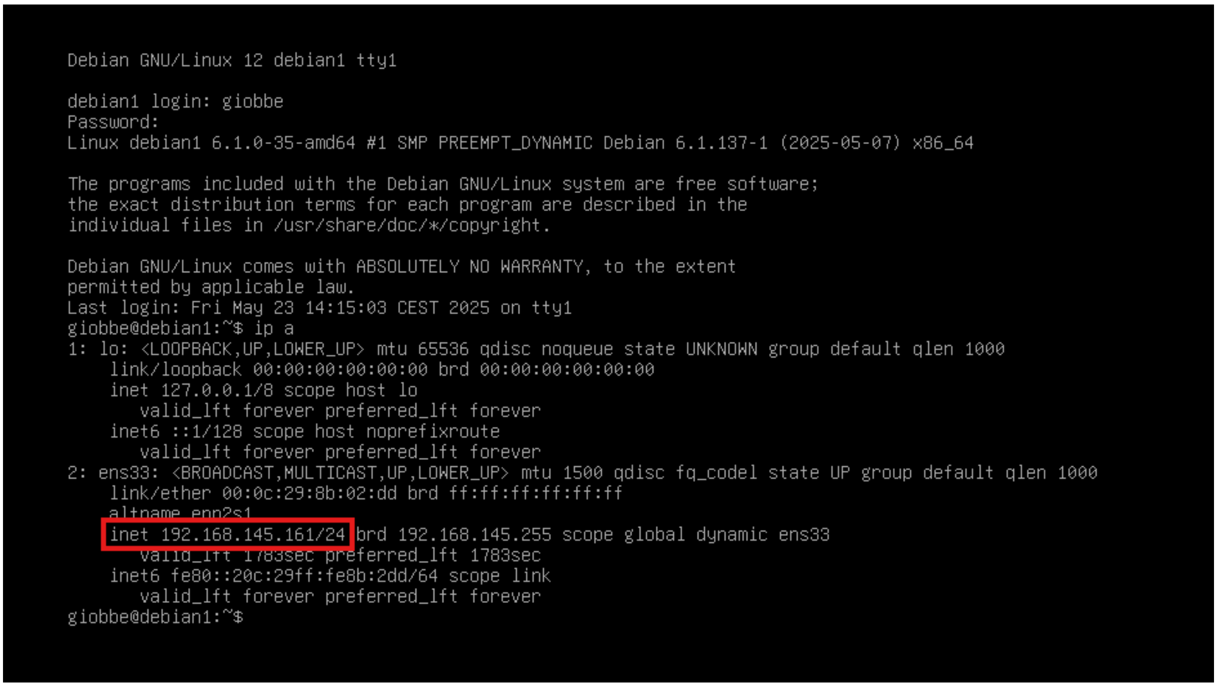
SSH

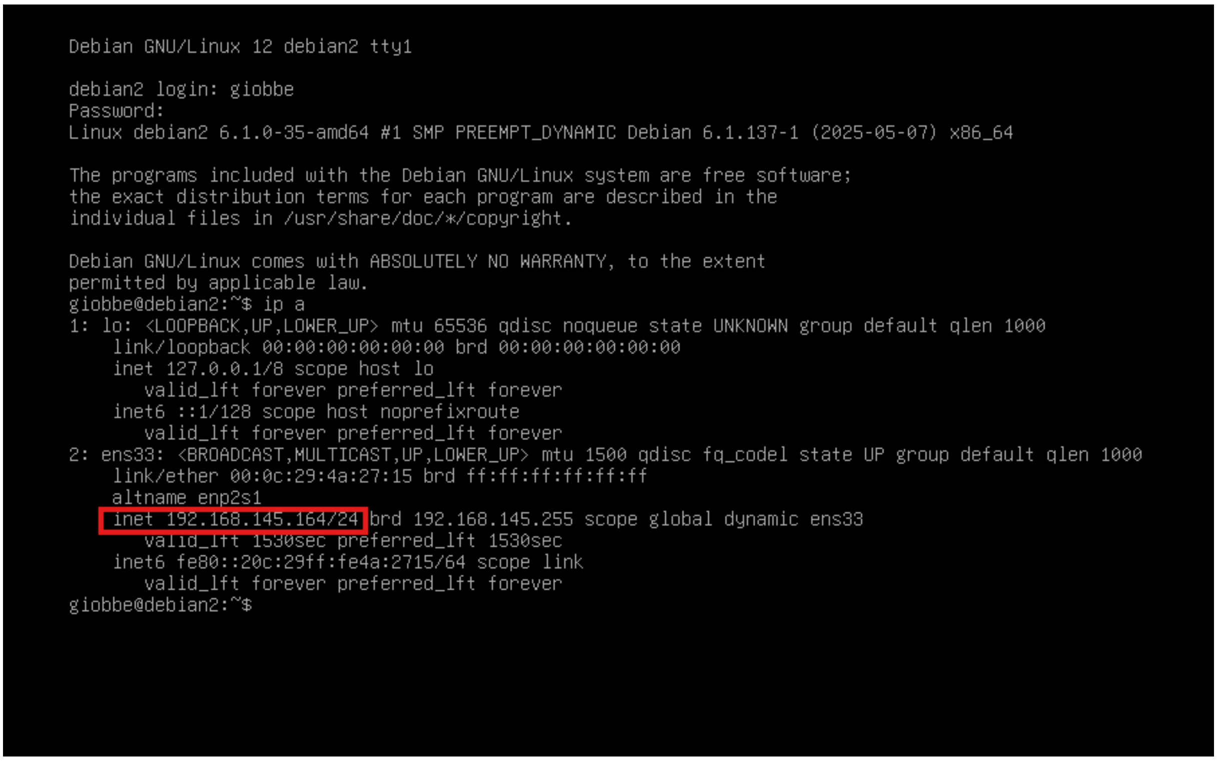
Étape 1 : Vérifier les adresses IP

Sur **debian1** (serveur) : ip a



```
Debian GNU/Linux 12 debian1 tty1

debian1 login: giobbe
Password:
Linux debian1 6.1.0-35-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.137-1 (2025-05-07) 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 May 23 14:15:03 CEST 2025 on tty1
giobbe@debian1:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:8b:02:dd brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.145.161/24 brd 192.168.145.255 scope global dynamic ens33
       valid_lft 1783sec preferred_lft 1783sec
    inet6 fe80::20c:29ff:fe8b:2dd/64 scope link
       valid_lft forever preferred_lft forever
giobbe@debian1:~$
```

Sur **debian2** (serveur) : ip a

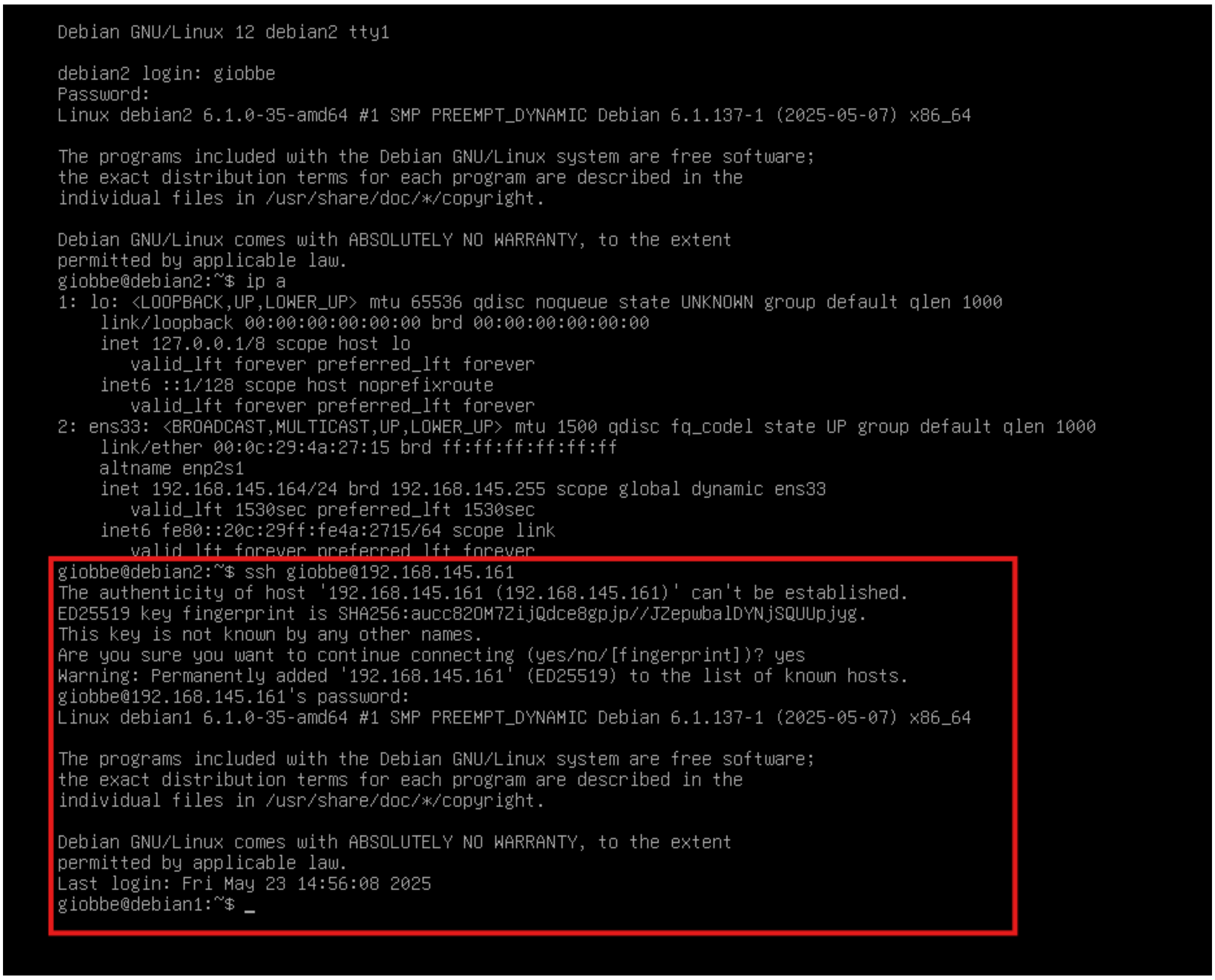


```
Debian GNU/Linux 12 debian2 tty1

debian2 login: giobbe
Password:
Linux debian2 6.1.0-35-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.137-1 (2025-05-07) 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.
giobbe@debian2:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:4a:27:15 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.145.164/24 brd 192.168.145.255 scope global dynamic ens33
       valid_lft 1530sec preferred_lft 1530sec
    inet6 fe80::20c:29ff:fe4a:2715/64 scope link
       valid_lft forever preferred_lft forever
giobbe@debian2:~$
```

Étape 2 : Teste la connexion SSH classique avec mot de passe

Sur la machine **client (debian2)** :

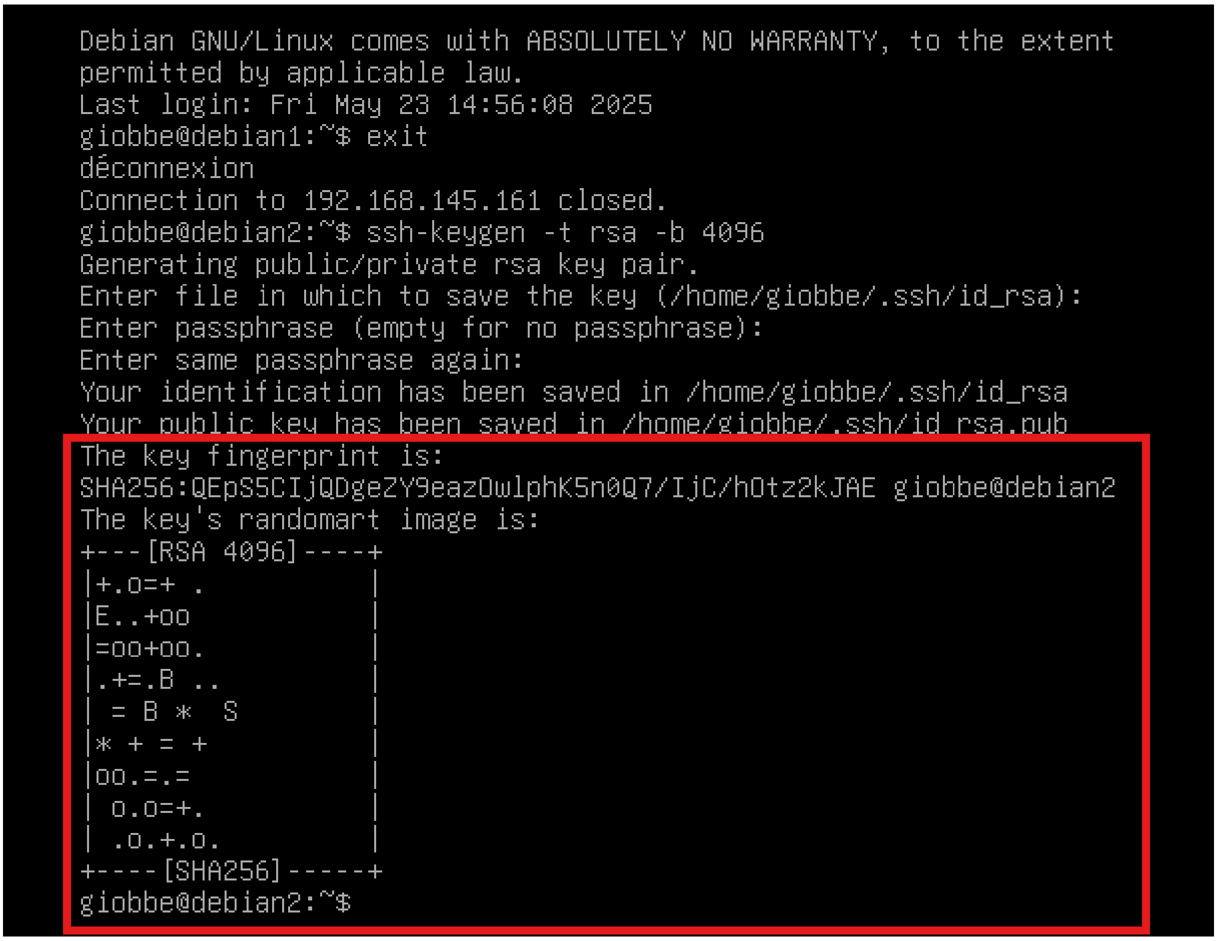
Il faut taper la commande : ssh giobbe@192.168.145.161 par l’IP réelle de debian1



```
Debian GNU/Linux 12 debian2 tty1

debian2 login: giobbe
Password:
Linux debian2 6.1.0-35-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.137-1 (2025-05-07) 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.
giobbe@debian2:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:4a:27:15 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.145.164/24 brd 192.168.145.255 scope global dynamic ens33
       valid_lft 1530sec preferred_lft 1530sec
    inet6 fe80::20c:29ff:fe4a:2715/64 scope link
       valid_lft forever preferred_lft forever
giobbe@debian2:~$ ssh giobbe@192.168.145.161
The authenticity of host '192.168.145.161 (192.168.145.161)' can't be established.
ED25519 key fingerprint is SHA256:aucc82OM7ZijQdce8gpjp//JZepwbalDYNjSQUUpjyg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.145.161' (ED25519) to the list of known hosts.
giobbe@192.168.145.161's password:
Linux debian1 6.1.0-35-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.137-1 (2025-05-07) 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 May 23 14:56:08 2025
giobbe@debian1:~$ _
```

Étape 3 : Générer une paire de clés SSH sur la machine client (debian2)

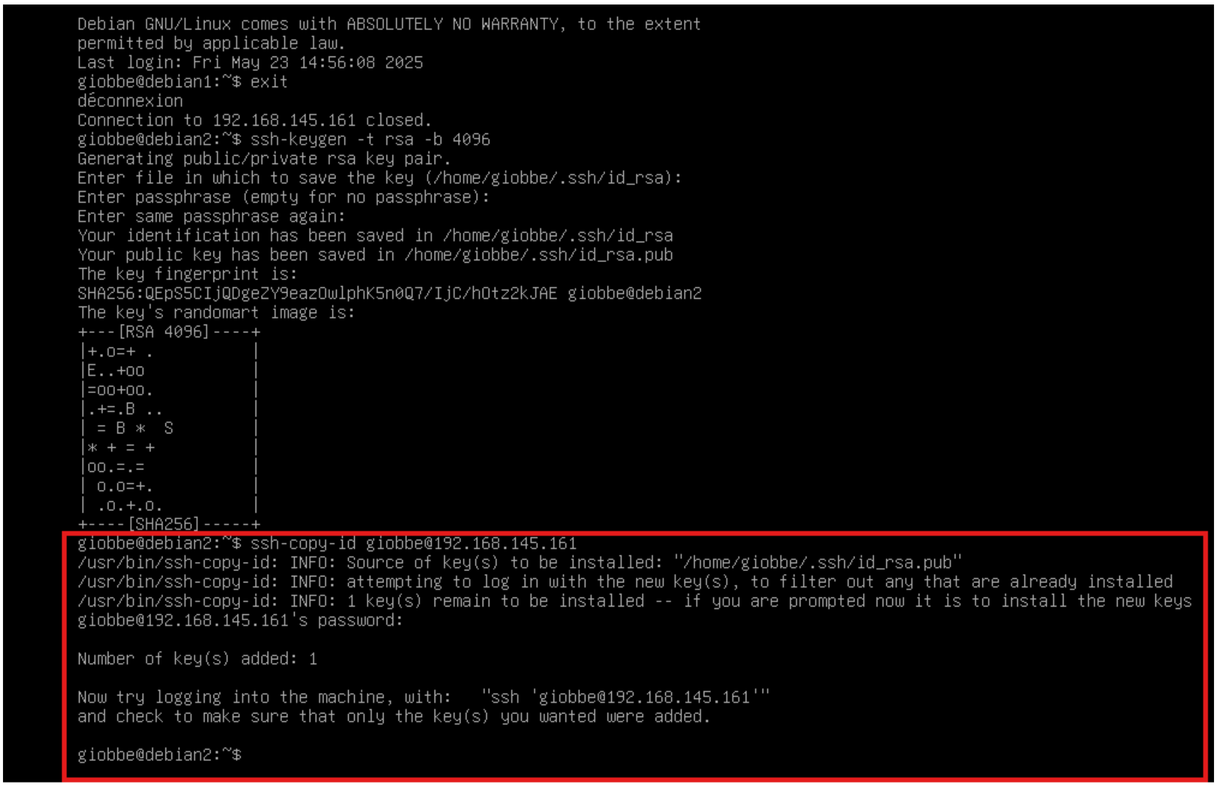
Sur debian2, il faut tape la commande : ssh-keygen -t rsa -b 4096



```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri May 23 14:56:08 2025
giobbe@debian1:~$ exit
déconnexion
Connection to 192.168.145.161 closed.
giobbe@debian2:~$ ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/home/giobbe/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/giobbe/.ssh/id_rsa
Your public key has been saved in /home/giobbe/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:QEpS5CIjQDgeZY9eazOwlphK5n0Q7/IjC/hOtz2kJAE giobbe@debian2
The key's randomart image is:
+---[RSA 4096]----+
|+.o=+ .          |
|E..+oo           |
|=oo+oo.          |
|.+=.B ..         |
| = B *  S        |
|* + = +          |
|oo.=.=           |
| o.o=+.          |
| .o.+.o.         |
+----[SHA256]-----+
giobbe@debian2:~$
```

Étape 4 : Copier la clé publique sur la machine serveur (debian1)

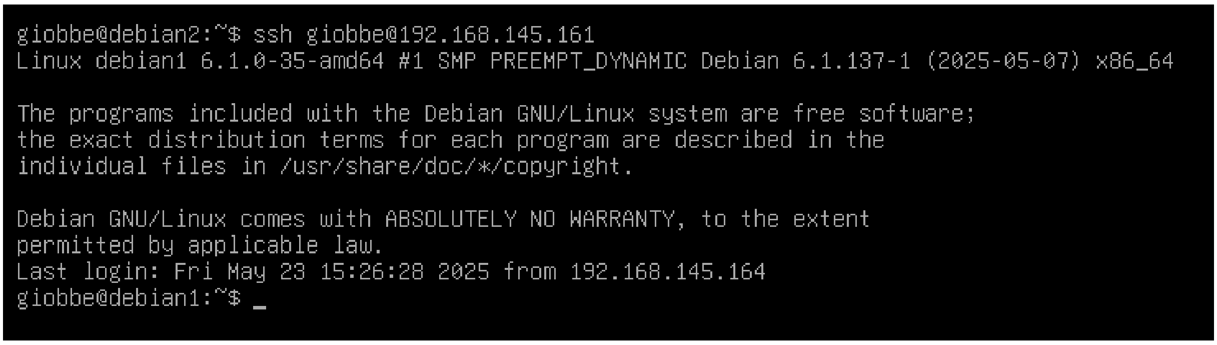
Sur debian2 (client) : ssh-copy-id giobbe@192.168.145.161



```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri May 23 14:56:08 2025
giobbe@debian1:~$ exit
déconnexion
Connection to 192.168.145.161 closed.
giobbe@debian2:~$ ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/home/giobbe/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/giobbe/.ssh/id_rsa
Your public key has been saved in /home/giobbe/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:QEpS5CIjQDgeZY9eazOwlphK5n0Q7/IjC/hOtz2kJAE giobbe@debian2
The key's randomart image is:
+---[RSA 4096]----+
|+.o=+ .          |
|E..+oo           |
|=oo+oo.          |
|.+=.B ..         |
| = B *  S        |
|* + = +          |
|oo.=.=           |
| o.o=+.          |
| .o.+.o.         |
+----[SHA256]-----+
giobbe@debian2:~$ ssh-copy-id giobbe@192.168.145.161
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/giobbe/.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 prompted now it is to install the new keys
giobbe@192.168.145.161's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'giobbe@192.168.145.161'"
and check to make sure that only the key(s) you wanted were added.

giobbe@debian2:~$
```

Étape 5 : Tester la connexion SSH sans mot de passe

Toujours sur debian2 tape : ssh giobbe@192.168.145.161

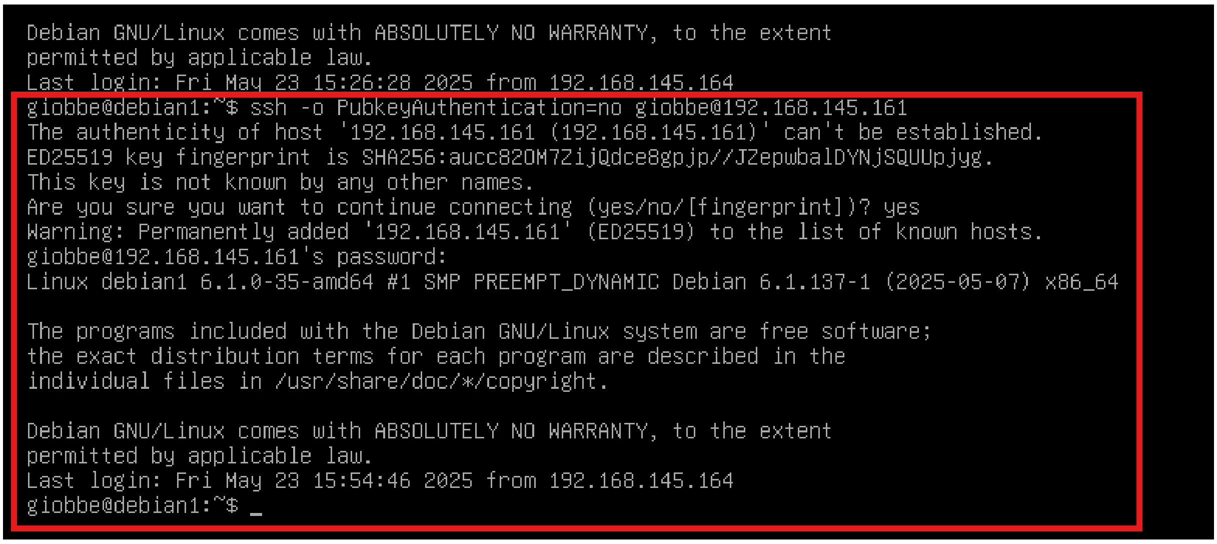


```
giobbe@debian2:~$ ssh giobbe@192.168.145.161
Linux debian1 6.1.0-35-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.137-1 (2025-05-07) x86_64

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 May 23 15:26:28 2025 from 192.168.145.164
giobbe@debian1:~$ _
```

Étape 6 : Forcer la connexion avec mot de passe (ignorer la clé)

Sur debian2 : ssh -o PubkeyAuthentication=no giobbe@192.168.145.161

- -o PubkeyAuthentication=no : ça dit au client SSH **de ne pas utiliser la clé SSH** pour s'authentifier.
- Du coup, la connexion passe par la méthode **mot de passe**.
- Le serveur va alors te demander ton mot de passe, même si la clé est configurée.

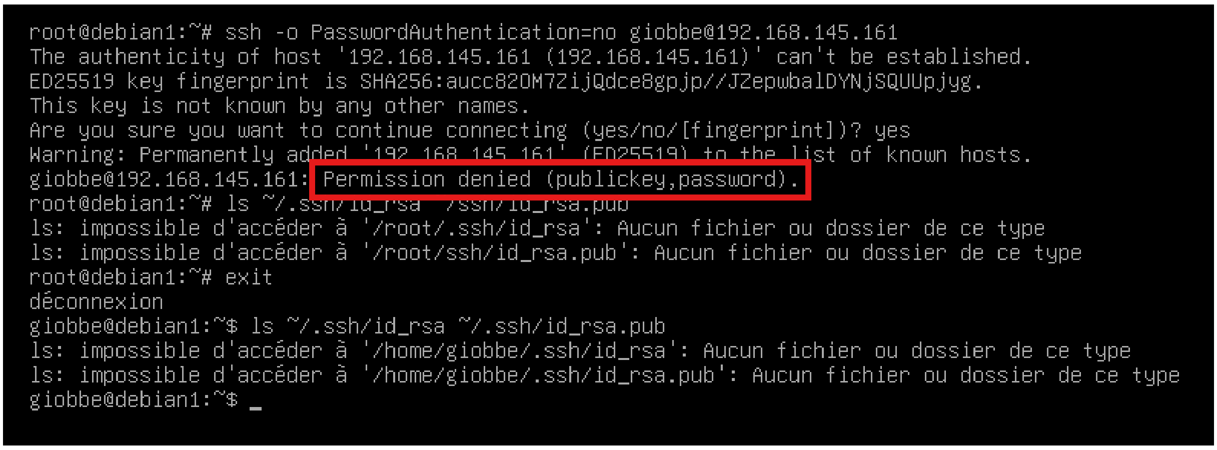


```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri May 23 15:26:28 2025 from 192.168.145.164
giobbe@debian1:~$ ssh -o PubkeyAuthentication=no giobbe@192.168.145.161
The authenticity of host '192.168.145.161 (192.168.145.161)' can't be established.
ED25519 key fingerprint is SHA256:aucc82OM7ZijQdce8gpjp//JZepwbalDYNjSQUUpjyg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.145.161' (ED25519) to the list of known hosts.
giobbe@192.168.145.161's password:
Linux debian1 6.1.0-35-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.137-1 (2025-05-07) 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 May 23 15:54:46 2025 from 192.168.145.164
giobbe@debian1:~$ _
```

Étape 7 : Forcer la connexion sans mot de passe (ignorer mot de passe)

Sur debian2 : ssh -o PasswordAuthentication=no giobbe@192.168.145.161

- L'option -o PasswordAuthentication=no signifie :
  « N'utilise **pas** la méthode mot de passe ».
- Donc, SSH essaiera uniquement la clé SSH.
- Si la clé ne correspond pas ou qu'elle n'existe pas sur le serveur, **la connexion échouera** (tu ne pourras pas te connecter).



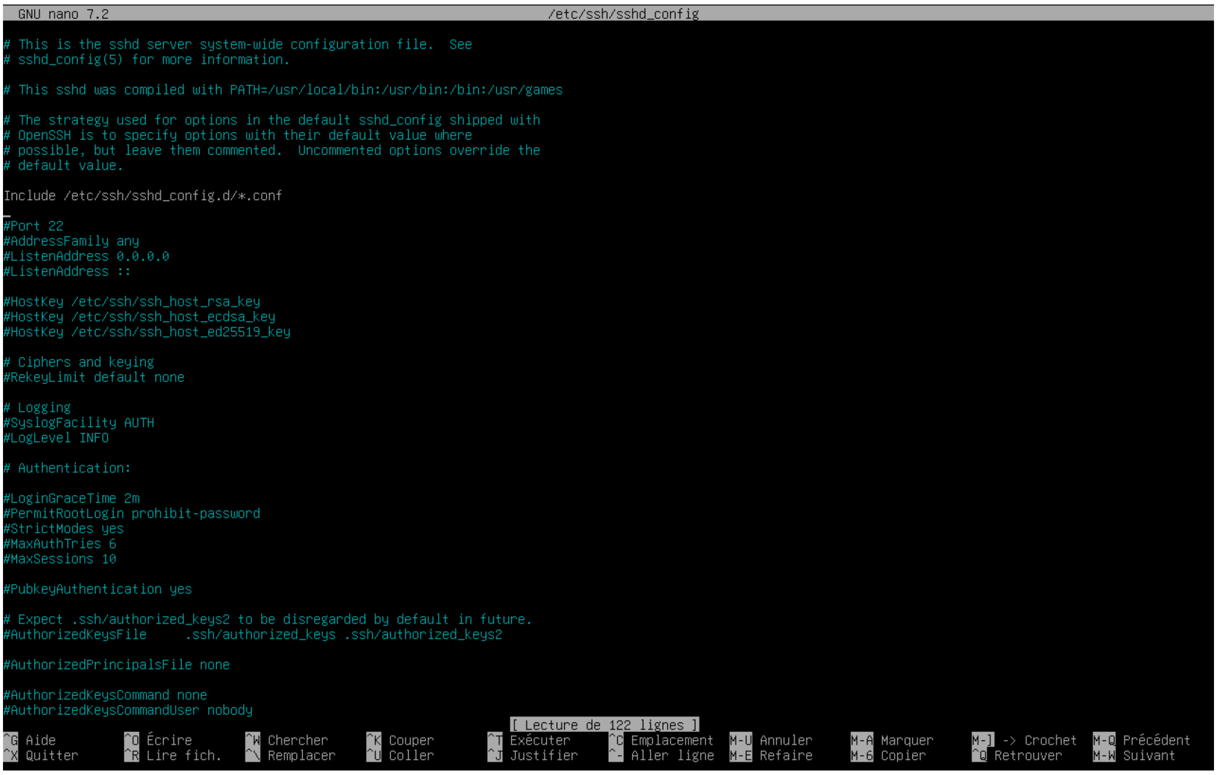
```
root@debian1:~# ssh -o PasswordAuthentication=no giobbe@192.168.145.161
The authenticity of host '192.168.145.161 (192.168.145.161)' can't be established.
ED25519 key fingerprint is SHA256:aucc82OM7ZijQdce8gpjp//JZepwbalDYNjSQUUpjyg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.145.161' (ED25519) to the list of known hosts.
giobbe@192.168.145.161: Permission denied (publickey,password).
root@debian1:~# ls ~/.ssh/id_rsa ~/ssh/id_rsa.pub
ls: impossible d'accéder à '/root/.ssh/id_rsa': Aucun fichier ou dossier de ce type
ls: impossible d'accéder à '/root/ssh/id_rsa.pub': Aucun fichier ou dossier de ce type
root@debian1:~# exit
déconnexion
giobbe@debian1:~$ ls ~/.ssh/id_rsa ~/.ssh/id_rsa.pub
ls: impossible d'accéder à '/home/giobbe/.ssh/id_rsa': Aucun fichier ou dossier de ce type
ls: impossible d'accéder à '/home/giobbe/.ssh/id_rsa.pub': Aucun fichier ou dossier de ce type
giobbe@debian1:~$ _
```

J'ai trouvé ce problème et j'obtiens la permission denied.

Ce n'est pas bon

Alors je cherche quel est le problème

Je fait : sudo nano /etc/ssh/sshd_config

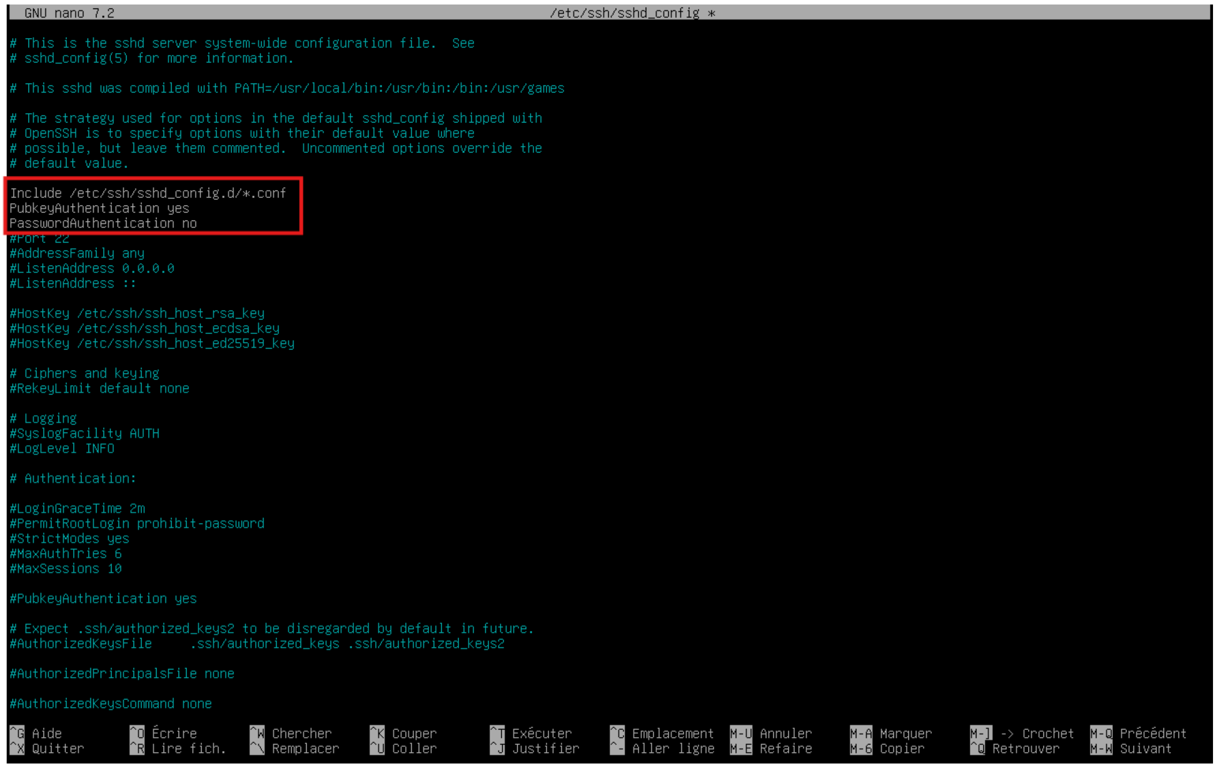


```
  GNU nano 7.2                                                            /etc/ssh/sshd_config

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

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

# 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 ::

#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
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile     .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody
                                                                  [ Lecture de 122 lignes ]
^G Aide         ^O Écrire       ^W Chercher     ^K Couper       ^T Exécuter     ^C Emplacement  M-U Annuler     M-A Marquer     M-] -> Crochet  M-Q Précédent
^X Quitter      ^R Lire fich.   ^\ Remplacer    ^U Coller       ^J Justifier    ^- Aller ligne  M-E Refaire     M-6 Copier      ^Q Retrouver    M-W Suivant
```

Et puis j'ai ajouté :

PubkeyAuthentication yes

PasswordAuthentication no

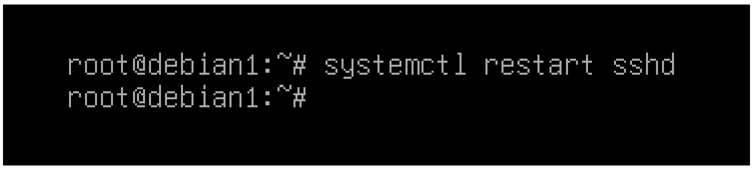


```
  GNU nano 7.2                                /etc/ssh/sshd_config *

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

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

# 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
PubkeyAuthentication yes
PasswordAuthentication no
#Port 22
#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

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

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

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile     .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
^G Aide       ^O Écrire     ^W Chercher   ^K Couper     ^T Exécuter   ^C Emplacement M-U Annuler   M-A Marquer   M-] -> Crochet M-Q Précédent
^X Quitter    ^R Lire fich. ^\ Remplacer  ^U Coller     ^J Justifier  ^/ Aller ligne M-E Refaire   M-6 Copier    ^Q Retrouver   M-W Suivant
```

J'ai sauvegardé et fermé:

- Dans **nano**, fais : Ctrl + O, puis Entrée pour enregistrer.
- Puis Ctrl + X pour quitter.

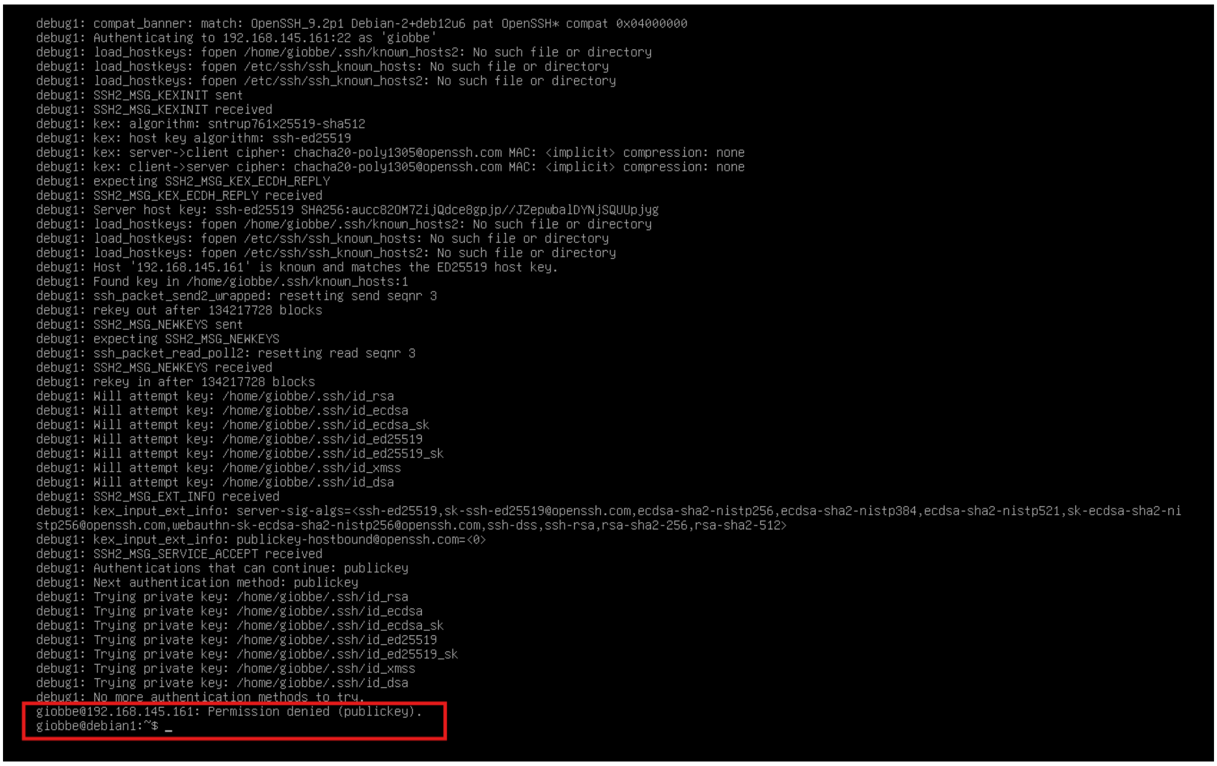
Redémarre le service SSH : sudo systemctl restart sshd



```
root@debian1:~# systemctl restart sshd
root@debian1:~#
```

Maintenant, testé la connexion depuis **Debian2 (le client)** :

ssh -v -o PasswordAuthentication=no giobbe@192.168.145.161



```
debug1: compat_banner: match: OpenSSH_9.2p1 Debian-2+deb12u6 pat OpenSSH* compat 0x04000000
debug1: Authenticating to 192.168.145.161:22 as 'giobbe'
debug1: load_hostkeys: fopen /home/giobbe/.ssh/known_hosts2: No such file or directory
debug1: load_hostkeys: fopen /etc/ssh/ssh_known_hosts: No such file or directory
debug1: load_hostkeys: fopen /etc/ssh/ssh_known_hosts2: No such file or directory
debug1: SSH2_MSG_KEXINIT sent
debug1: SSH2_MSG_KEXINIT received
debug1: kex: algorithm: sntrup761x25519-sha512
debug1: kex: host key algorithm: ssh-ed25519
debug1: kex: server->client cipher: chacha20-poly1305@openssh.com MAC: <implicit> compression: none
debug1: kex: client->server cipher: chacha20-poly1305@openssh.com MAC: <implicit> compression: none
debug1: expecting SSH2_MSG_KEX_ECDH_REPLY
debug1: SSH2_MSG_KEX_ECDH_REPLY received
debug1: Server host key: ssh-ed25519 SHA256:aucc82OM7ZijQdce8gpjp//JZepwbalDYNjSQUUpjyg
debug1: load_hostkeys: fopen /home/giobbe/.ssh/known_hosts2: No such file or directory
debug1: load_hostkeys: fopen /etc/ssh/ssh_known_hosts: No such file or directory
debug1: load_hostkeys: fopen /etc/ssh/ssh_known_hosts2: No such file or directory
debug1: Host '192.168.145.161' is known and matches the ED25519 host key.
debug1: Found key in /home/giobbe/.ssh/known_hosts:1
debug1: ssh_packet_send2_wrapped: resetting send seqnr 3
debug1: rekey out after 134217728 blocks
debug1: SSH2_MSG_NEWKEYS sent
debug1: expecting SSH2_MSG_NEWKEYS
debug1: ssh_packet_read_poll2: resetting read seqnr 3
debug1: SSH2_MSG_NEWKEYS received
debug1: rekey in after 134217728 blocks
debug1: Will attempt key: /home/giobbe/.ssh/id_rsa
debug1: Will attempt key: /home/giobbe/.ssh/id_ecdsa
debug1: Will attempt key: /home/giobbe/.ssh/id_ecdsa_sk
debug1: Will attempt key: /home/giobbe/.ssh/id_ed25519
debug1: Will attempt key: /home/giobbe/.ssh/id_ed25519_sk
debug1: Will attempt key: /home/giobbe/.ssh/id_xmss
debug1: Will attempt key: /home/giobbe/.ssh/id_dsa
debug1: SSH2_MSG_EXT_INFO received
debug1: kex_input_ext_info: server-sig-algs=<ssh-ed25519,sk-ssh-ed25519@openssh.com,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,sk-ecdsa-sha2-ni
stp256@openssh.com,webauthn-sk-ecdsa-sha2-nistp256@openssh.com,ssh-dss,ssh-rsa,rsa-sha2-256,rsa-sha2-512>
debug1: kex_input_ext_info: publickey-hostbound@openssh.com=<0>
debug1: SSH2_MSG_SERVICE_ACCEPT received
debug1: Authentications that can continue: publickey
debug1: Next authentication method: publickey
debug1: Trying private key: /home/giobbe/.ssh/id_rsa
debug1: Trying private key: /home/giobbe/.ssh/id_ecdsa
debug1: Trying private key: /home/giobbe/.ssh/id_ecdsa_sk
debug1: Trying private key: /home/giobbe/.ssh/id_ed25519
debug1: Trying private key: /home/giobbe/.ssh/id_ed25519_sk
debug1: Trying private key: /home/giobbe/.ssh/id_xmss
debug1: Trying private key: /home/giobbe/.ssh/id_dsa
debug1: No more authentication methods to try.
giobbe@192.168.145.161: Permission denied (publickey).
giobbe@debian1:~$ _
```

Cette fois, nous n'avons que le problème (publickey)

Je fait : ssh -vvv -o PasswordAuthentication=no giobbe@192.168.145.161

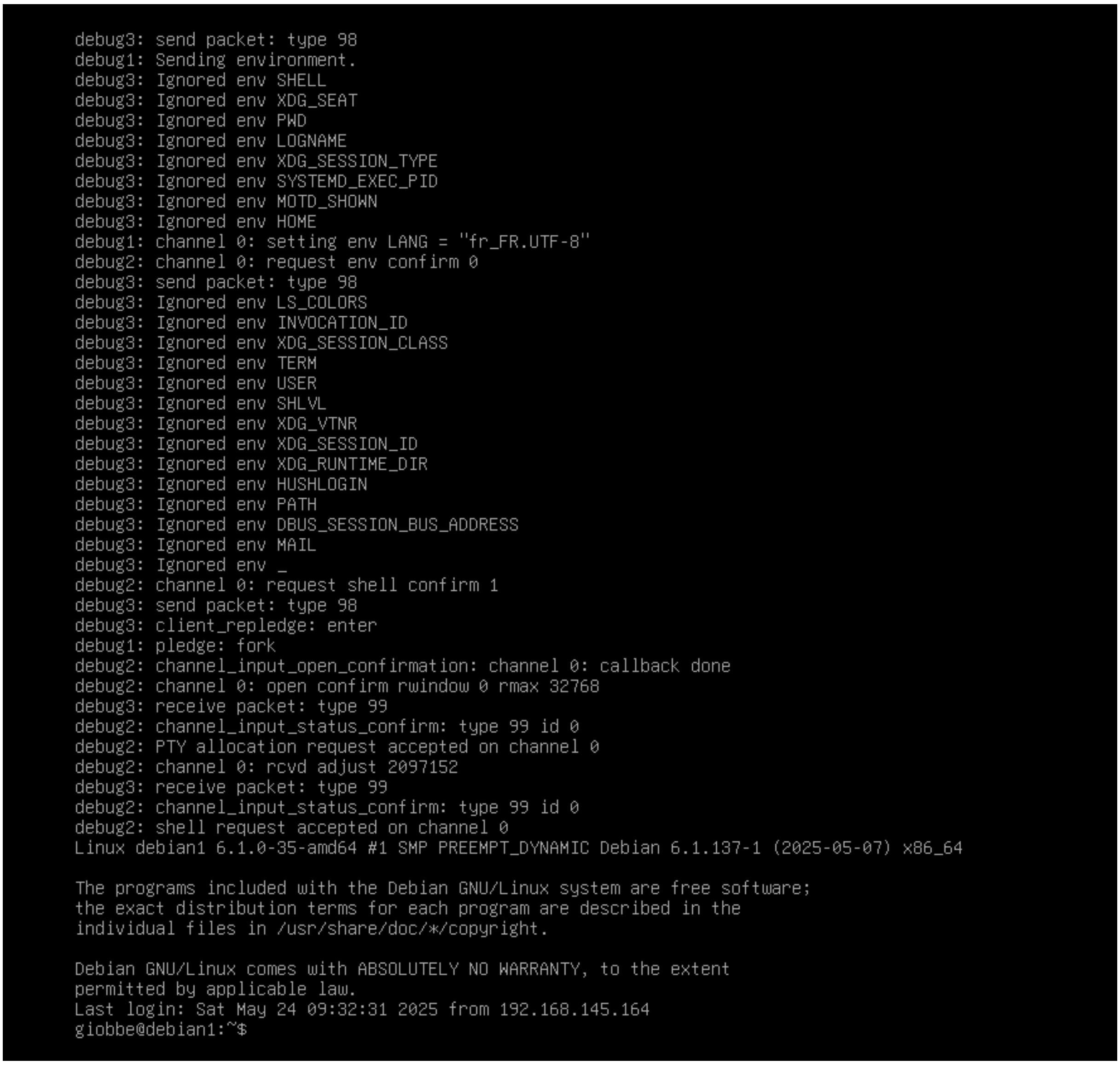
Résultat de la commande :

Last login: Sat May 24 09:32:31 2025 from 192.168.145.164

Et juste avant,

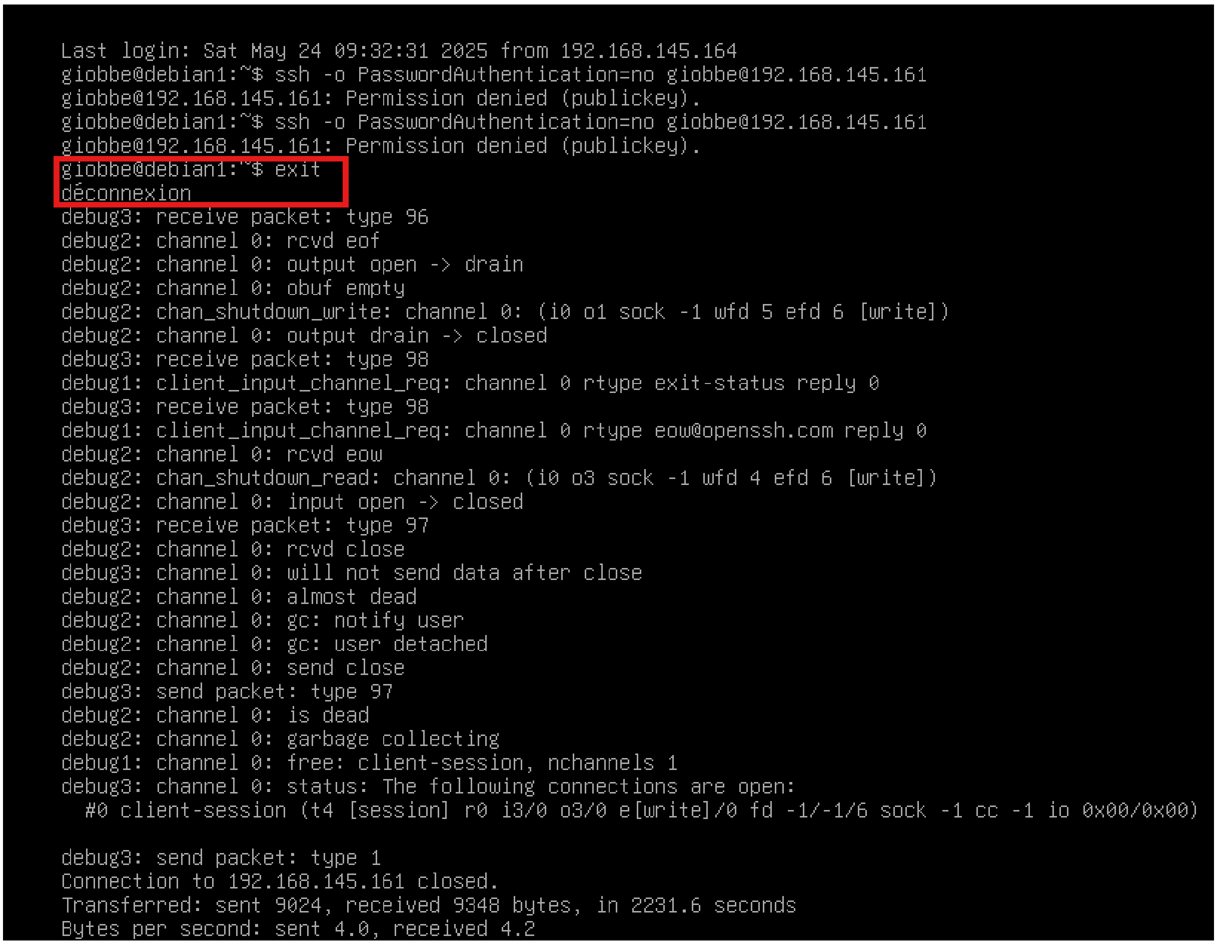
shell request accepted on channel 0

Ça signifie que **le serveur a accepté la clé publique**, j'ai donné un shell, et je suis maintenant connecté sur **Debian1 (le serveur) sans mot de passe**.



```
debug3: send packet: type 98
debug1: Sending environment.
debug3: Ignored env SHELL
debug3: Ignored env XDG_SEAT
debug3: Ignored env PWD
debug3: Ignored env LOGNAME
debug3: Ignored env XDG_SESSION_TYPE
debug3: Ignored env SYSTEMD_EXEC_PID
debug3: Ignored env MOTD_SHOWN
debug3: Ignored env HOME
debug1: channel 0: setting env LANG = "fr_FR.UTF-8"
debug2: channel 0: request env confirm 0
debug3: send packet: type 98
debug3: Ignored env LS_COLORS
debug3: Ignored env INVOCATION_ID
debug3: Ignored env XDG_SESSION_CLASS
debug3: Ignored env TERM
debug3: Ignored env USER
debug3: Ignored env SHLVL
debug3: Ignored env XDG_VTNR
debug3: Ignored env XDG_SESSION_ID
debug3: Ignored env XDG_RUNTIME_DIR
debug3: Ignored env HUSHLOGIN
debug3: Ignored env PATH
debug3: Ignored env DBUS_SESSION_BUS_ADDRESS
debug3: Ignored env MAIL
debug3: Ignored env _
debug2: channel 0: request shell confirm 1
debug3: send packet: type 98
debug3: client_repledge: enter
debug1: pledge: fork
debug2: channel_input_open_confirmation: channel 0: callback done
debug2: channel 0: open confirm rwindow 0 rmax 32768
debug3: receive packet: type 99
debug2: channel_input_status_confirm: type 99 id 0
debug2: PTY allocation request accepted on channel 0
debug2: channel 0: rcvd adjust 2097152
debug3: receive packet: type 99
debug2: channel_input_status_confirm: type 99 id 0
debug2: shell request accepted on channel 0
Linux debian1 6.1.0-35-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.137-1 (2025-05-07) 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: Sat May 24 09:32:31 2025 from 192.168.145.164
giobbe@debian1:~$
```

Maintenant je quitte Debian1 avec la commande : exit



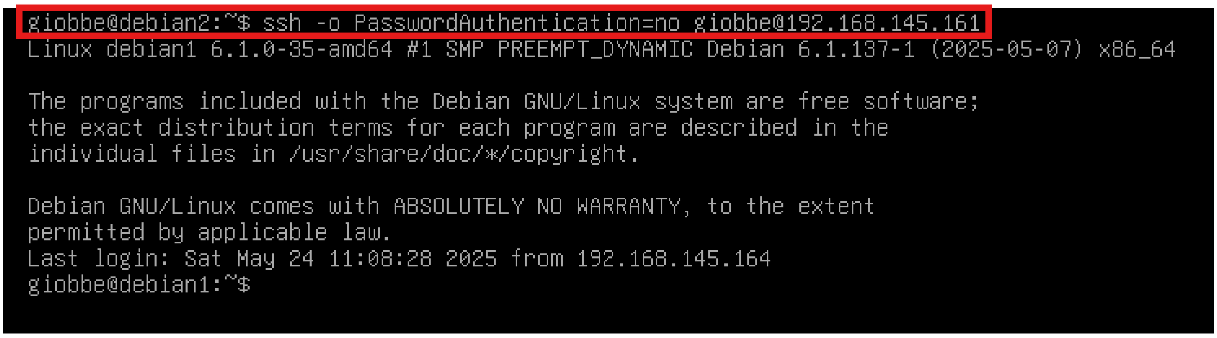
```
Last login: Sat May 24 09:32:31 2025 from 192.168.145.164
giobbe@debian1:~$ ssh -o PasswordAuthentication=no giobbe@192.168.145.161
giobbe@192.168.145.161: Permission denied (publickey).
giobbe@debian1:~$ ssh -o PasswordAuthentication=no giobbe@192.168.145.161
giobbe@192.168.145.161: Permission denied (publickey).
giobbe@debian1:~$ exit
déconnexion
debug3: receive packet: type 96
debug2: channel 0: rcvd eof
debug2: channel 0: output open -> drain
debug2: channel 0: obuf empty
debug2: chan_shutdown_write: channel 0: (i0 o1 sock -1 wfd 5 efd 6 [write])
debug2: channel 0: output drain -> closed
debug3: receive packet: type 98
debug1: client_input_channel_req: channel 0 rtype exit-status reply 0
debug3: receive packet: type 98
debug1: client_input_channel_req: channel 0 rtype eow@openssh.com reply 0
debug2: channel 0: rcvd eow
debug2: chan_shutdown_read: channel 0: (i0 o3 sock -1 wfd 4 efd 6 [write])
debug2: channel 0: input open -> closed
debug3: receive packet: type 97
debug2: channel 0: rcvd close
debug3: channel 0: will not send data after close
debug2: channel 0: almost dead
debug2: channel 0: gc: notify user
debug2: channel 0: gc: user detached
debug2: channel 0: send close
debug3: send packet: type 97
debug2: channel 0: is dead
debug2: channel 0: garbage collecting
debug1: channel 0: free: client-session, nchannels 1
debug3: channel 0: status: The following connections are open:
  #0 client-session (t4 [session] r0 i3/0 o3/0 e[write]/0 fd -1/-1/6 sock -1 cc -1 io 0x00/0x00)

debug3: send packet: type 1
Connection to 192.168.145.161 closed.
Transferred: sent 9024, received 9348 bytes, in 2231.6 seconds
Bytes per second: sent 4.0, received 4.2
```

Retour à debian2 (client) et je tape :

ssh -vvv -o PasswordAuthentication=no giobbe@192.168.145.161

Pour s'assurer que cela fonctionne

Procédure fonctionnelle.



```
giobbe@debian2:~$ ssh -o PasswordAuthentication=no giobbe@192.168.145.161
Linux debian1 6.1.0-35-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.137-1 (2025-05-07) 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: Sat May 24 11:08:28 2025 from 192.168.145.164
giobbe@debian1:~$
```

Objectif : Ajouter deux paramètres supplémentaires

Étape 1 : Édite le fichier de configuration SSH

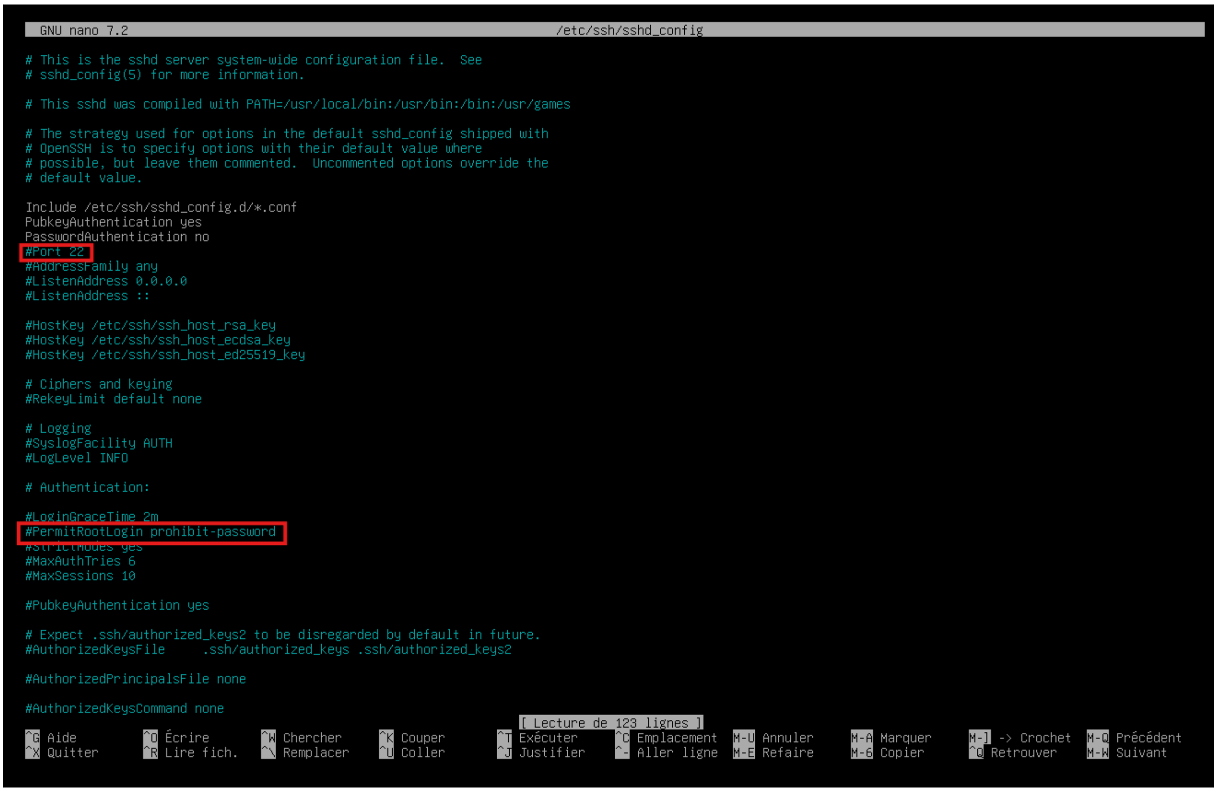
sudo nano /etc/ssh/sshd_config (debian1) (cote server) sudo nano /etc/ssh/sshd_config

On va

Décommenter ces lignes (en retirant #)

Et modifier comme ceci :

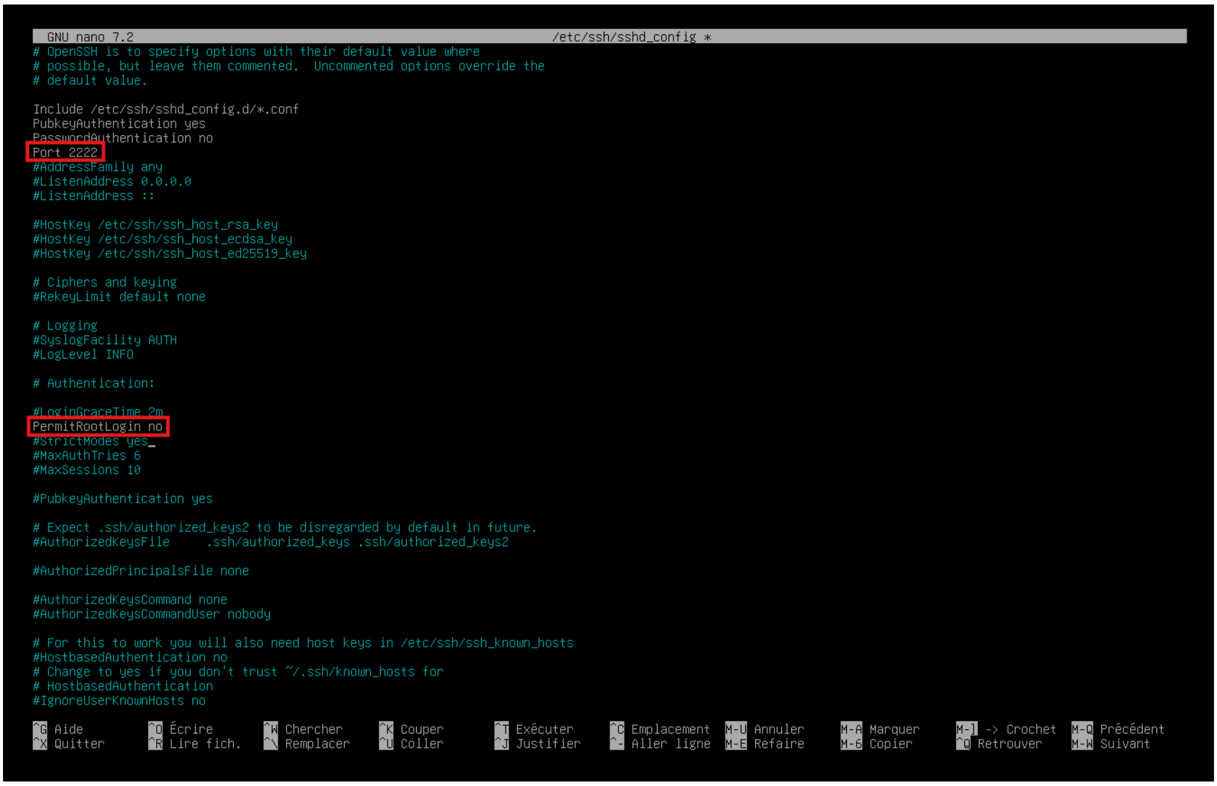
- Port 2222
- PermitRootLogin no



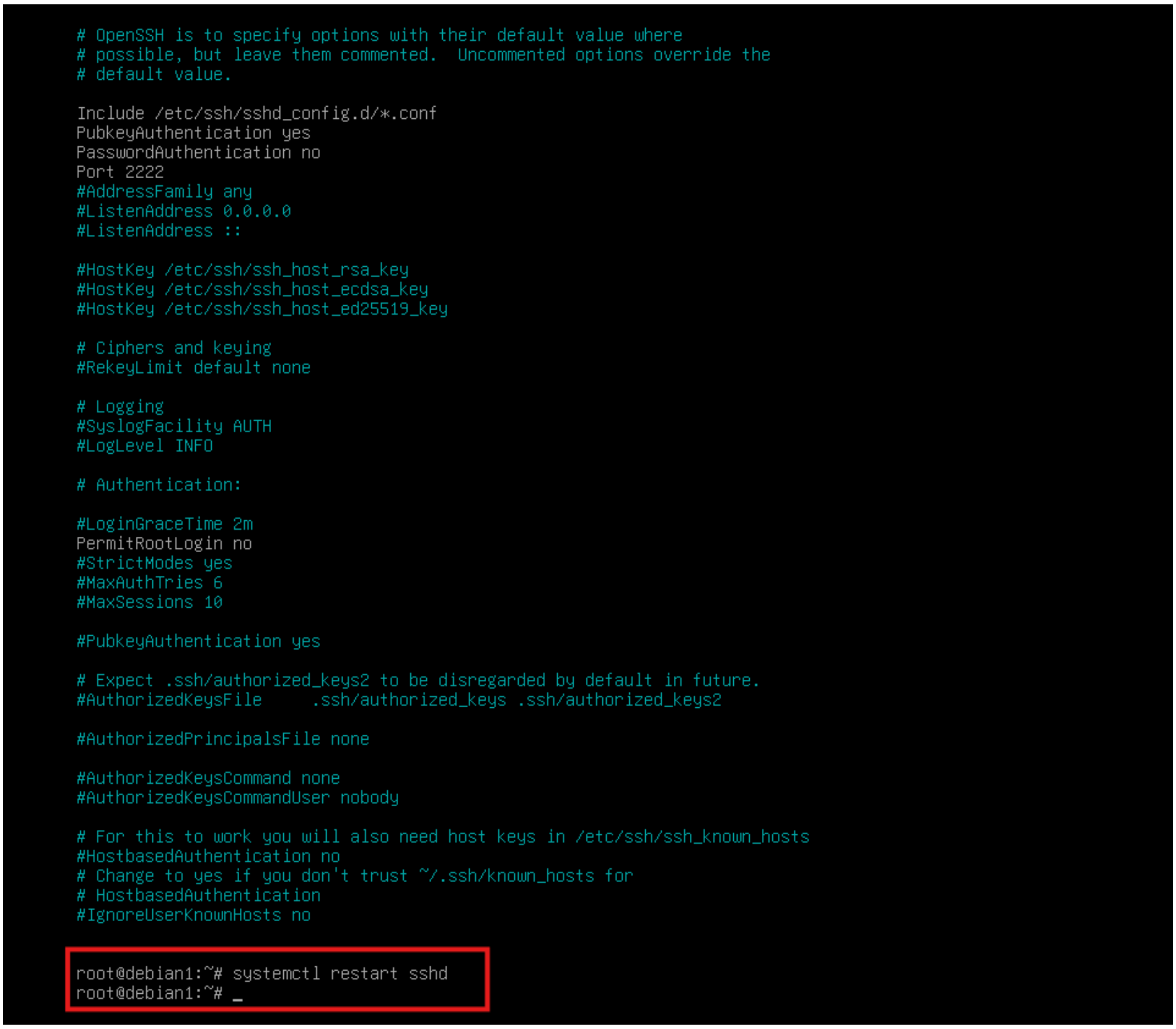
```
  GNU nano 7.2                                                      /etc/ssh/sshd_config
# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

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

# 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
PubkeyAuthentication yes
PasswordAuthentication no
#Port 22
#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

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

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

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile     .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
                                                                [ Lecture de 123 lignes ]
^G Aide        ^O Écrire      ^W Chercher    ^K Couper      ^T Exécuter    ^C Emplacement M-U Annuler     M-A Marquer     M-] -> Crochet  M-Q Précédent
^X Quitter     ^R Lire fich.  ^\ Remplacer   ^U Coller      ^J Justifier   ^- Aller ligne M-E Refaire     M-6 Copier      ^Q Retrouver    M-W Suivant
```

Ctrl o + Enter +Ctrl x

Apres Sauvegarde + Redémarrage : sudo systemctl restart sshd



```
  GNU nano 7.2                                                          /etc/ssh/sshd_config *
# 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
PubkeyAuthentication yes
PasswordAuthentication no
Port 2222
#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

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes_
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# 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_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
^G Aide         ^O Écrire       ^W Chercher     ^K Couper       ^T Exécuter     ^C Emplacement  M-U Annuler     M-A Marquer     M-] -> Crochet  M-Q Précédent
^X Quitter      ^R Lire fich.   ^\ Remplacer    ^U Coller       ^J Justifier    ^_ Aller ligne  M-E Refaire     M-6 Copier      ^Q Retrouver    M-W Suivant
```

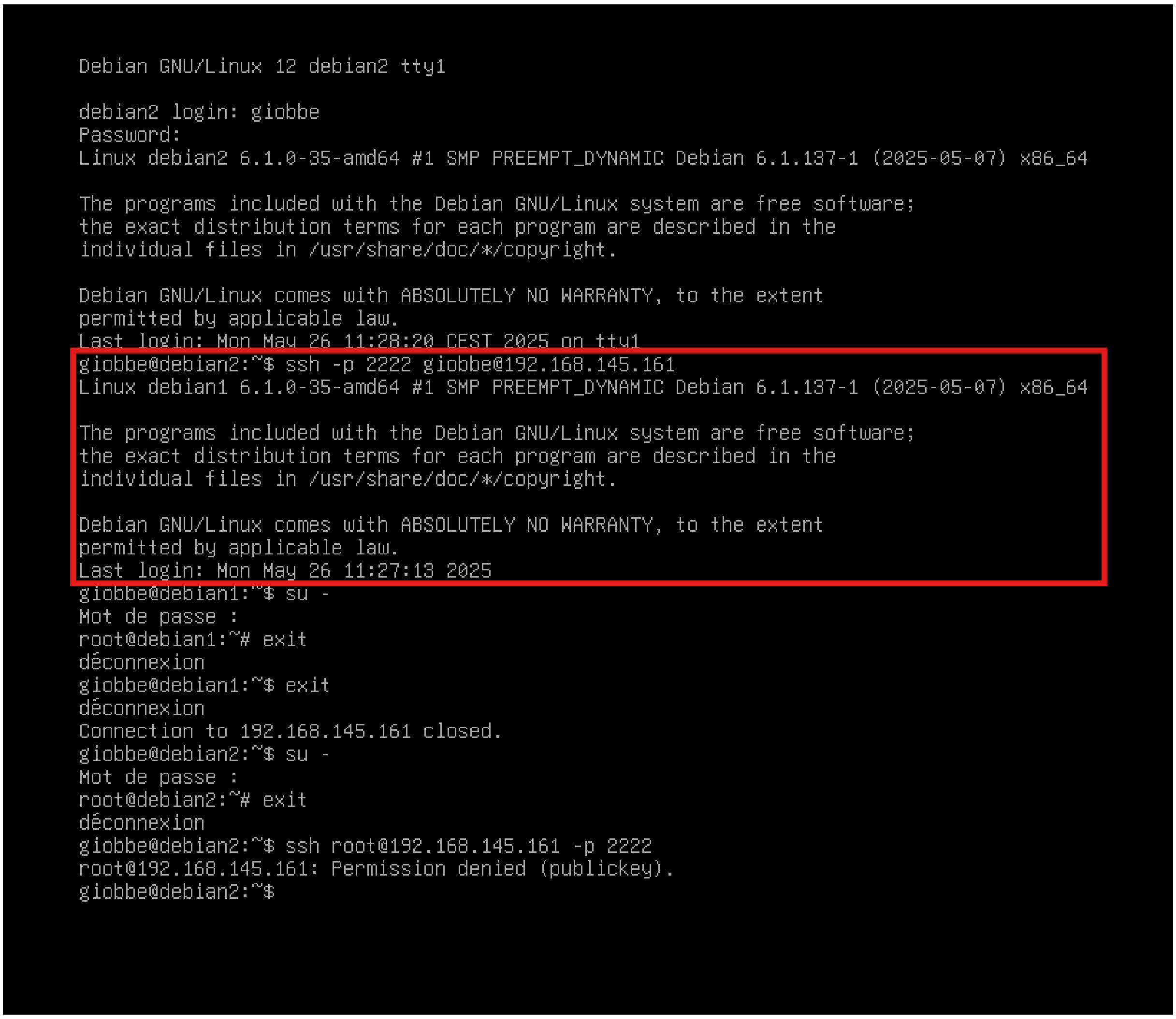


```
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf
PubkeyAuthentication yes
PasswordAuthentication no
Port 2222
#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

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# 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_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no

root@debian1:~# systemctl restart sshd
root@debian1:~# _
```

Test côté client

Depuis Debian2 (client), connection avec le nouveau port :

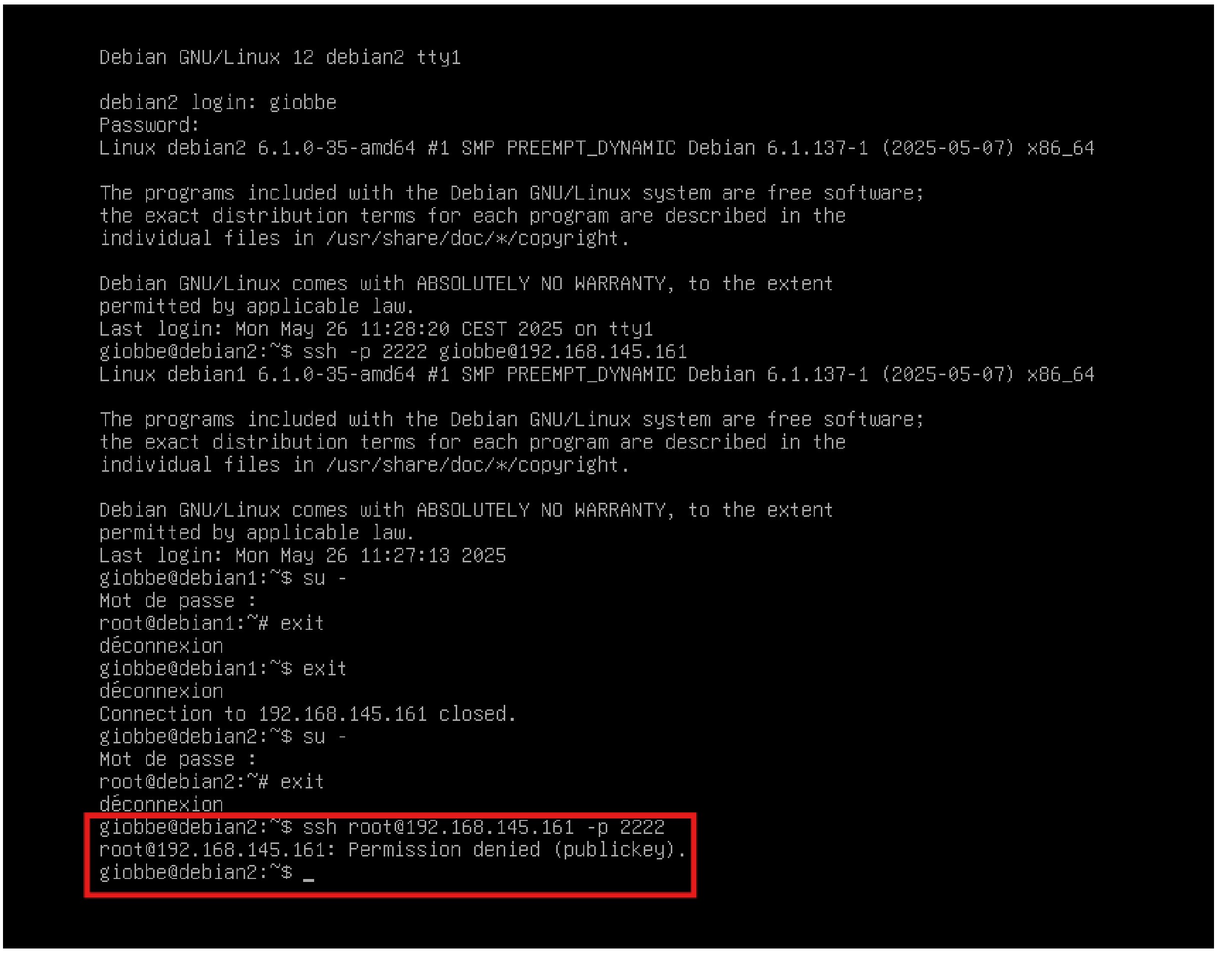
ssh -p 2222 giobbe@192.168.145.161



```
Debian GNU/Linux 12 debian2 tty1

debian2 login: giobbe
Password:
Linux debian2 6.1.0-35-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.137-1 (2025-05-07) 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: Mon May 26 11:28:20 CEST 2025 on tty1
giobbe@debian2:~$ ssh -p 2222 giobbe@192.168.145.161
Linux debian1 6.1.0-35-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.137-1 (2025-05-07) 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: Mon May 26 11:27:13 2025
giobbe@debian1:~$ su -
Mot de passe :
root@debian1:~# exit
déconnexion
giobbe@debian1:~$ exit
déconnexion
Connection to 192.168.145.161 closed.
giobbe@debian2:~$ su -
Mot de passe :
root@debian2:~# exit
déconnexion
giobbe@debian2:~$ ssh root@192.168.145.161 -p 2222
root@192.168.145.161: Permission denied (publickey).
giobbe@debian2:~$
```

Apres on teste que la connexion en root est refusée :

ssh root@192.168.145.161 -p 2222



```
Debian GNU/Linux 12 debian2 tty1

debian2 login: giobbe
Password:
Linux debian2 6.1.0-35-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.137-1 (2025-05-07) 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: Mon May 26 11:28:20 CEST 2025 on tty1
giobbe@debian2:~$ ssh -p 2222 giobbe@192.168.145.161
Linux debian1 6.1.0-35-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.137-1 (2025-05-07) 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: Mon May 26 11:27:13 2025
giobbe@debian1:~$ su -
Mot de passe :
root@debian1:~# exit
déconnexion
giobbe@debian1:~$ exit
déconnexion
Connection to 192.168.145.161 closed.
giobbe@debian2:~$ su -
Mot de passe :
root@debian2:~# exit
déconnexion
giobbe@debian2:~$ ssh root@192.168.145.161 -p 2222
root@192.168.145.161: Permission denied (publickey).
giobbe@debian2:~$ _
```

Permission denied (publickey)

Cela signifie que :

- Le client a tenté de se connecter **en tant que root**.
- Le serveur **refuse toute connexion SSH au compte root**, même avec une clé publique.
- Le paramètre PermitRootLogin no est donc **correctement appliqué**.

Conclusion

Cet exercice m’a permis de comprendre et de mettre en pratique les différents modes de connexion SSH entre un client et un serveur.
J’ai appris à :

- Établir une connexion SSH classique avec mot de passe,
- Mettre en place une authentification par clé publique avec ou sans passphrase,
- Forcer l'utilisation ou l'interdiction d'une méthode d’authentification,
- Modifier les paramètres du serveur SSH pour renforcer la sécurité, comme le changement de port et l’interdiction de connexion en root.

Grâce à cette configuration, le serveur est maintenant mieux protégé contre les accès non autorisés et les attaques automatisées.