

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
```

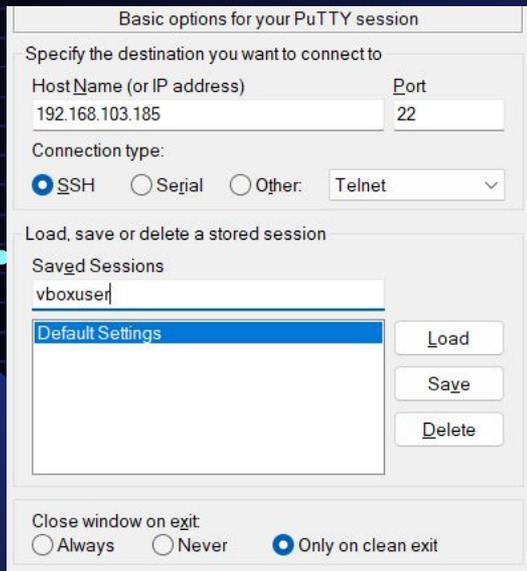
installer ssh

Tout simplement faire apt install openssh-server pour installer 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



The image shows the PuTTY configuration window titled "Basic options for your PuTTY session". It is divided into several sections:

- Specify the destination you want to connect to:** Host Name (or IP address) is "192.168.103.185" and Port is "22".
- Connection type:** SSH is selected with a radio button. Other options are Serial and Other: Telnet.
- Load, save or delete a stored session:** A list of saved sessions contains "vboxuser|". "Default Settings" is selected and highlighted in blue. Buttons for "Load", "Save", and "Delete" are visible.
- Close window on exit:** "Only on clean exit" is selected with a radio button. Other options are "Always" and "Never".



```
vboxuser@samba: ~  
login as: vboxuser  
vboxuser@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: Thu Feb  1 11:52:04 2024 from 192.168.204.7  
vboxuser@samba:~$
```

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

```
user@samba: ~
GNU nano 5.4 /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

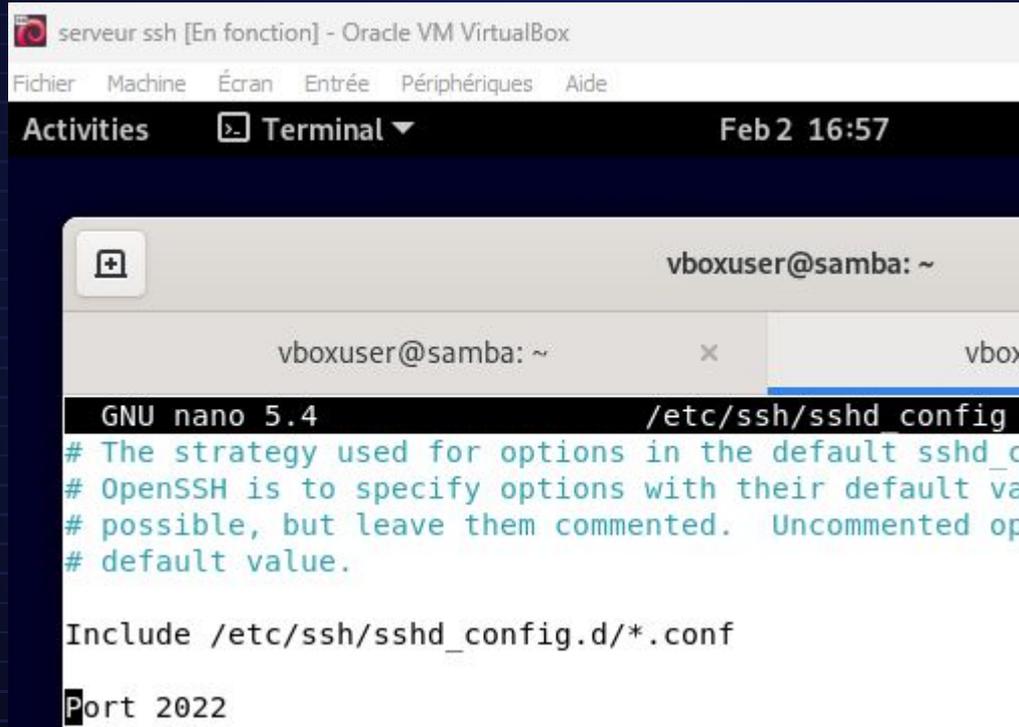
# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

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

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
[ File '/etc/ssh/sshd_config' is unwritable ]
^G Help      ^O Write Out  ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File  ^_ Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

changer le port



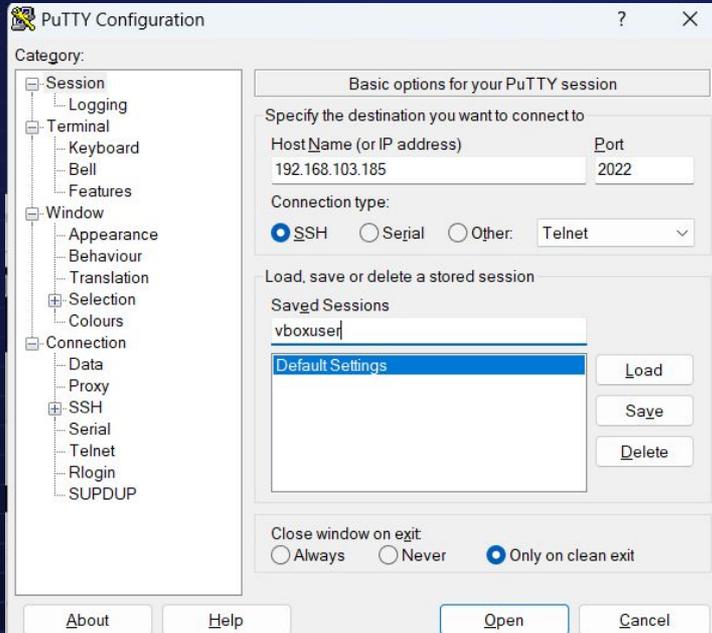
```
serveur ssh [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
Activities Terminal Feb 2 16:57
vboxuser@samba: ~
GNU nano 5.4 /etc/ssh/sshd config
# The strategy used for options in the default sshd_c
# OpenSSH is to specify options with their default va
# possible, but leave them commented. Uncommented op
# default value.

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

Port 2022
```

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

```
#LoginGraceTime 2m  
PermitRootLogin yes
```

```
login as: root  
root@192.168.202.185's password:  
Linux samba 5.10.0-27-amd64 #1 SMP De  
  
The programs included with the Debian  
the exact distribution terms for each  
individual files in /usr/share/doc/*/
```

ge Debian GNU/Linux comes with ABSOLUTELY
permitted by applicable law.
root@samba:~#



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

Car si on 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

```
# To disable tunneled clear
#PasswordAuthentication yes
PermitEmptyPasswords yes
```



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 crée 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+CZL80dJcN+1WmBaJQ root@vierge
The key's randomart image is:
+----[DSA 1024]-----+
|      .oo o++o .. |
|      ...+o+E .. |
|      =++ = B .. |
|    o o.= X = .. |
|      S = 0 + + |
|      + = 0 = |
|    o . = o |
|      . . |
```

Gérer l'échange des clés publiques

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

```
root@viere:~# cat ~/.ssh/id_dsa
-----BEGIN OPENSSH PRIVATE KEY-----
o3BlbnZaC1rZXKtdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeb0AAAAAGAAAABCKadCIM4
vS6cR0JbQonLS6AAAAEAAAAEAAAGxAAAAB3NzaC1kc3MAAACBAIJmLjxxZ2mdNU7I2Fm
sA0I304SK4+Lm4g4bquRR02P47vuT9yF3Mvg74KkrtqPbsk1oLnI0gppqTfQWX/MdXy/t
s4e0+HrnIuPw4KFfXDrjc3adB/C2Q2PVxq//02h3y9z44+72uRFIryVlNeehYzNuHHbjlX
KbZxY4feykDDAAAAAFQDwt7bKHWL2g5c19CjBT3YcVzQEmQAAAIAYxx4Cws3ReDmFaT0qUL
v+z08N9+Ihzt5b3DMMARAu+YWFRXkSlhqm2v0F1ctEtFGT1Y7nraVC8Gi2xT9vZnGN3Y1o
Xd0FHhJnIUI7zJXRfSbtMuJuBQJJYqCqC3e0lvliRqzX3EAHN7b2U7jZlfcAv46cdB4C
D0rjl4A2CMzAAAAIBQlfgawggy7nfBmSyHeJVHoeF15iMwWg0GeppXQ9VJbMz+WbA4V7XU
lqMoLxHp3H7Fh55tU6Yqqc1JyKrgnRrG2/nUG6AUBLf3mAB+zu0PFPMXzND0/25WfNyoG4
22TBCs+Nwt0X0oXGCZ0xDcwR5I95GLscuvZ0fPw6Q0FS06CQAAEdx5ZyJ1hN93nwj8Syw
Z0jceRplc/94cp/vDcGdQfCukSHUBFdrG+6AIAFecRpAnnd7jUwLzIXbnnBlX94xuWqMso
tYsa6DmV2vWkyKNl8KKGKMMjQy6MwU9tn3stWXIUTJQYBLG7e9P/kJLY0vSdbM8Gmt8KDQ
0B+836nXsIQ5MwzP84Xfqs0lnWetNqRXWltzaESb5xMK2M37JZy9Tm0jYHALHcuIeEWjE
t5NKhUw0vIHjklambcDZ06RrR4yBZ0BSlvNKzqpS0HnlnZBf0BCugvyM42z/mBTEvt/UL8
emZkZPuL0wnHSL4iGxldovpULs8vj4g2m5rgpMkySasT4069Phkwo3CI/EfAfBv74JE65
tdcBdaobpVYdjyPLPZI7J2PbfaQg0wrVKDpxc6N5e2T6r3EqTbWiLKVYxU1JxMW61Eohaa
AvPosfi/TM5W34V1JLXPSjdAUSuuAtADgrqgh/7T5J9VAuYzCznLbptNE0iXGKTKNyayef
PQl+YsIGIR8ldxdP43TfV9YVceky8T23P19VcR8N4+fqd8W2ltfKV3SVYkdm7Aes0u1ZB
lqfnN2FiIVPqMrp4KLO+oGNfAV0cf40+Q14ZwdoWJrjwzSDnoPkWfEmliFZGcwY=
-----END OPENSSH PRIVATE KEY-----
```

```
root@viere:~# cat ~/.ssh/id_dsa.pub
ssh-dss AAAAB3NzaC1kc3MAAACBAIJmLjxxZ2mdNU7I2FmLsA0I304SK4+Lm4g4bquRR02P47vuT9y
F3Mvg74KkrtqPbsk1oLnI0gppqTfQWX/MdXy/ts4e0+HrnIuPw4KFfXDrjc3adB/C2Q2PVxq//02h3y9
z44+72uRFIryVlNeehYzNuHHbjlXKbZxY4feykDDAAAAAFQDwt7bKHWL2g5c19CjBT3YcVzQEmQAAAIAY
xx4Cws3ReDmFaT0qULv+z08N9+Ihzt5b3DMMARAu+YWFRXkSlhqm2v0F1ctEtFGT1Y7nraVC8Gi2xT9v
ZnGN3Y1oXd0FHhJnIUI7zJXRfSbtMuJuBQJJYqCqC3e0lvliRqzX3EAHN7b2U7jZlfcAv46cdB4CD0
rjl4A2CMzAAAAIBQlfgawggy7nfBmSyHeJVHoeF15iMwWg0GeppXQ9VJbMz+WbA4V7XU1qMoLxHp3H7F
h55tU6Yqqc1JyKrgnRrG2/nUG6AUBLf3mAB+zu0PFPMXzND0/25WfNyoG422TBCs+Nwt0X0oXGCZ0xDc
wR5I95GLscuvZ0fPw6Q0FS06CQ== root@viere
```



**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.pub"
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/SbhpiZbKg5vvwHXyDhJXaA0V5+jsxrh1bUdeVXJh05vvHj6t
52miG4SlVFWVdjrjsh0pS6I9kz6ZT3BcITxbWwfHwM/v4cNdXQq9KBA4V1TMwq2x8VJFeeAsVt6XEG1f
q6bnnVSeRSroBcKxDVNpM1XDmShbaUe00QZoGauDAAAAFQD1U4eEH2FX3cludXVPuHcFZQvcHwAAAI EA
j7N9g0+ZsgreSFpFX/paI6U0Z+bFkSMGC4Bho/YB2oC05PVnNT824Kg80ijnIYtUPhoKV6IxMi69FrIO
XIQY8CgKqCsnwSkjzV0KbulUmFL+pinVzcYRKVNxPgPAdfve7KhJdNL/VSipPedkNXT04X0o2JBBeVX0
f5iqLH3+WkYAAACAK5i+9KV3oSNlfX0kF1YxVh+TVJ0fqQR+HbUoLaLoPnxiUYv6LsG7l2hLxHn8PWZW
3GMd0CaMxNCFfBykFnQnLNrrAxd2UjxWTLxjR+Pr3n8k2zXjs5Z8yH6wL5/Iqtth3BLLABiC5J3C81U2
e+0pbw8U7oJwdREtys0aWAtr16Y= root@samba
ssh-dss AAAAB3NzaC1kc3MAAACBAMoFwdJMKrT/noay8YoJK9FVq2rbLN3GPo/46Q+qCrpparoZ8eEe
1Gg84hFmKa/rWHvlyEazoDqZkVxI0K1koDju0ospCYANyBRHcl3FYTvmhjVTtC7Ec/naRxL9QWc3UHmQ
rIiDKVJQJQdC2woFhNf55Su727ZeqmZjHMPUH9QbnAAAAFQDpZfVYkK0HHUkKy+RJS6ZLwdjuvWAAAIEA
gP6Qa8D0gtiW+1tTDs9LYjiscewl/7EfuABbULITKe5mplfCKnE5PayfPj06cISyUJShA8cT0fWbH1w0
jW2+gMh0yGj9TYcMWY43APSCVA00u2s8R01IdHKJB+VHqrCojXD4tegxesMjQ/Yo/FdKaPjA6A2UxIPS
5+16FjBJ040AAACAB/Ne7RgC4xARvJzKv0WT9Q99Whfll+rLSkNTLlcsDz4F5jujb1KS2Q0vqXhs+Yr5
CASGxxBUt0akAr10IAwDRbYzpe/8V2ADG/ita07tl6uHl1eTExs0aX0H+fiNszvXUXIUPFdD/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

```
root@vierge:~# ssh user1@192.168.1.61
user1@192.168.1.61'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: Sat Feb 10 12:47:38 2024 from 192.168.1.62
```

9173	3152.9395115...	192.168.1.62	192.168.1.61
9174	3152.9395749...	192.168.1.61	192.168.1.62
9175	3152.9397685...	192.168.1.61	192.168.1.62
9176	3152.9399777...	192.168.1.61	192.168.1.62
9177	3152.9401724...	192.168.1.61	192.168.1.62
9178	3152.9406206...	192.168.1.62	192.168.1.61
9179	3152.9420363...	192.168.1.61	192.168.1.62
9180	3152.9432101...	192.168.1.62	192.168.1.61
9181	3152.9985423...	192.168.1.61	192.168.1.62
9182	3153.0157991...	192.168.1.61	192.168.1.62
9183	3153.0165268...	192.168.1.62	192.168.1.61

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

```
#ListenAddress 0.0.0.0
#ListenAddress ::
AllowGroups root ssh
PasswordAuthentication no
#HostKey /etc/ssh/ssh host r
```

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

(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@viierge:/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@viierge:/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
```