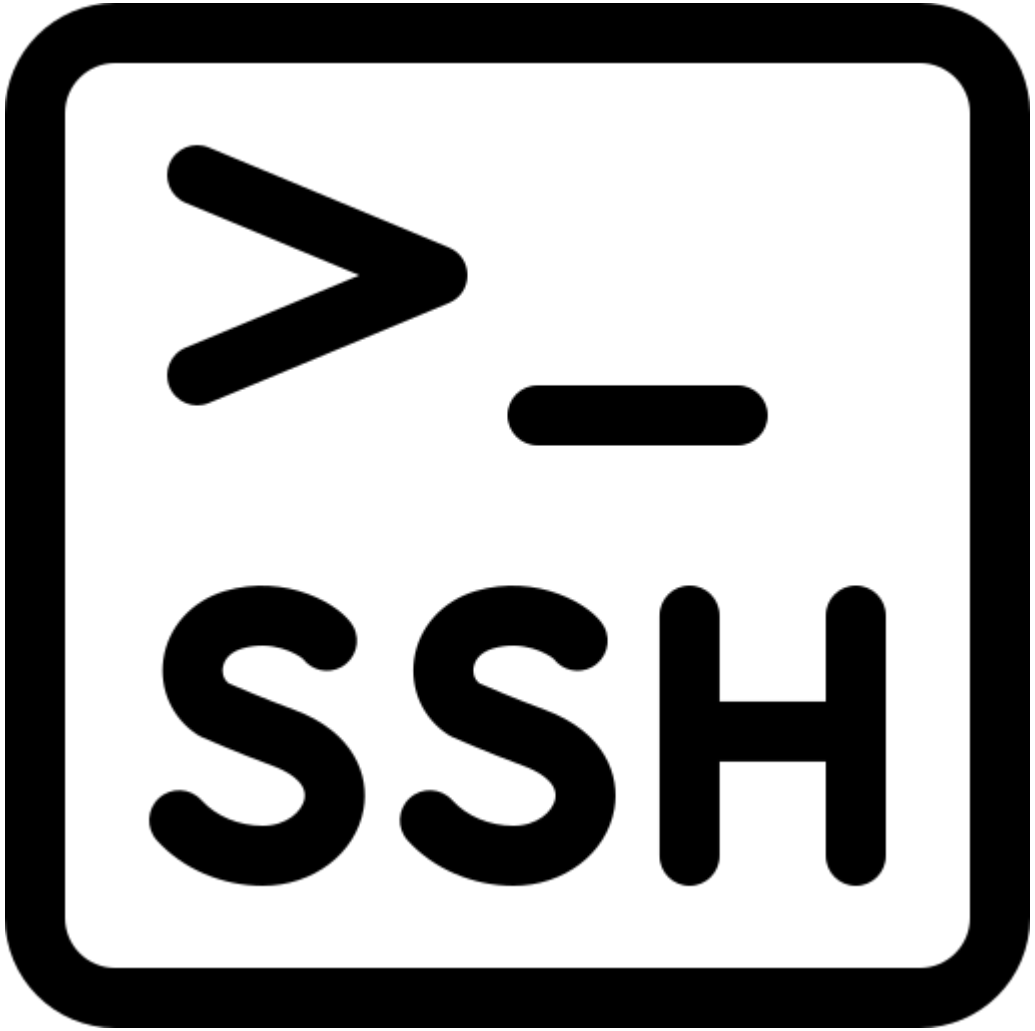


TP-Admin à distance: SSH

THOMAS GRZESINSKI

SSH qu’est que c’est ?

Secure Shell (SSH) est à la fois un programme informatique et un protocole de communication sécurisé permettant entre autre de se connecter à un ordinateur à distance.

CONFIGURATION DU SERVEUR

Installation du serveur SSH

Tout d'abord nous devons faire une update des paquets avec la *commande sudo apt-get update*

Ensuite installer le serveur avec la *commande apt install openssh-server*

Vérifier l'installation avec la *commande which ssh*

Si votre machine répond /usr/bin/ssh c'est que le serveur est correctement installé

```
root@thomas:~# which ssh
/usr/bin/ssh
```

Création des users

Tout d'abords il vous faut créer des user qui permettront de vous connecter a distance:

En *mode su – entrer la commande adduser + nomutilisateur*

Ici nous allons créer les users : users1 users2 et users3

Pour ajouter un utilisateur a un groupe utiliser la *commande addgroup + nom du groupe*

Nous allons créer le groupe ssh qui nous permettra d'autoriser les utilisateurs de ce groupe a se connecter a distance

Pour ajouter un utilisateur a un groupe il suffit d'entrer la *commande usermod –a –G nomgroupe nomutilisateur*

```
root@thomas:~# usermod -a -G etudiants user1
root@thomas:~# usermod -a -G etudiants user3
root@thomas:~# usermod -a -G ssh user1
root@thomas:~# usermod -a -G ssh user2
```

Changer le mot de passe

Pour une question de sécurité le meilleur choix à faire est de modifier les mots de passe de vos users (12 caractères minium, caractères spéciaux, lettres , chiffres)

Pour faire ceci utiliser la *commande passwd* quand vous êtes connectés à chaque utilisateur et entrer un nouveau mot de passe

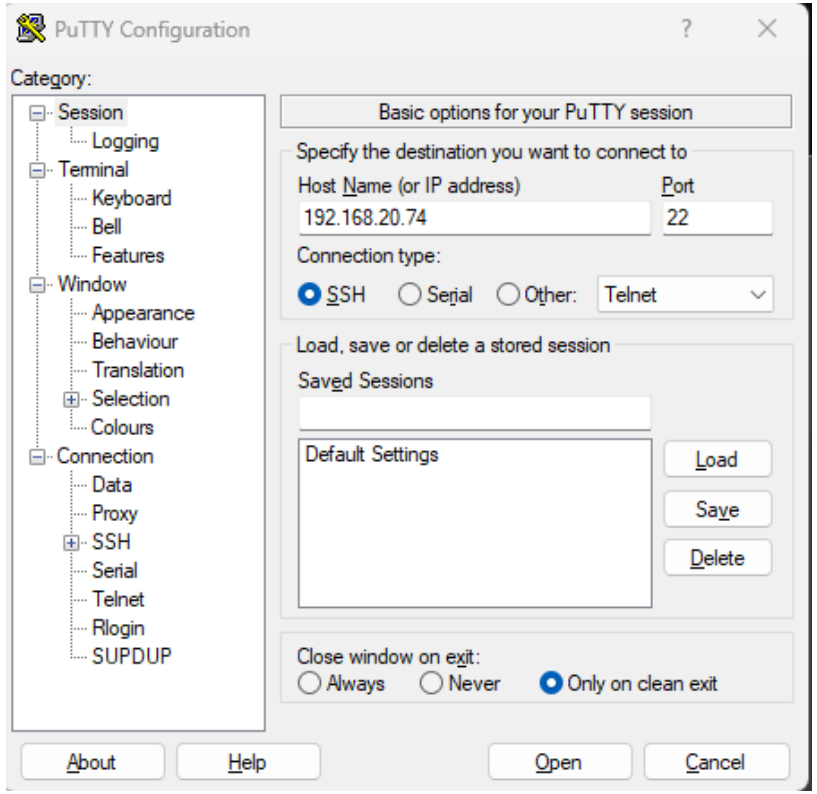
```
root@thomas:/home# passwd
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd : mot de passe mis à jour avec succès
```

Tentative de connexion à distance

Nous allons maintenant essayer de nous connecter à distance sur le serveur à l'aide de PUTTY (émulateur de terminal doublé d'un client pour les protocoles SSH, Telnet, rlogin et TCP brut)

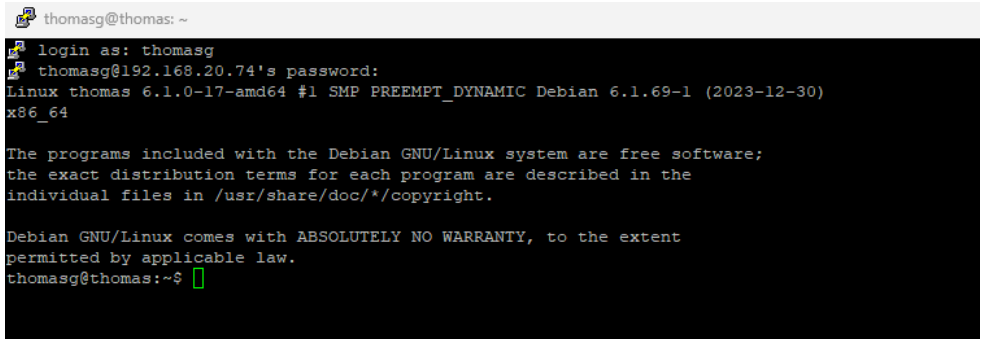
Avec une autre machine de type Windows

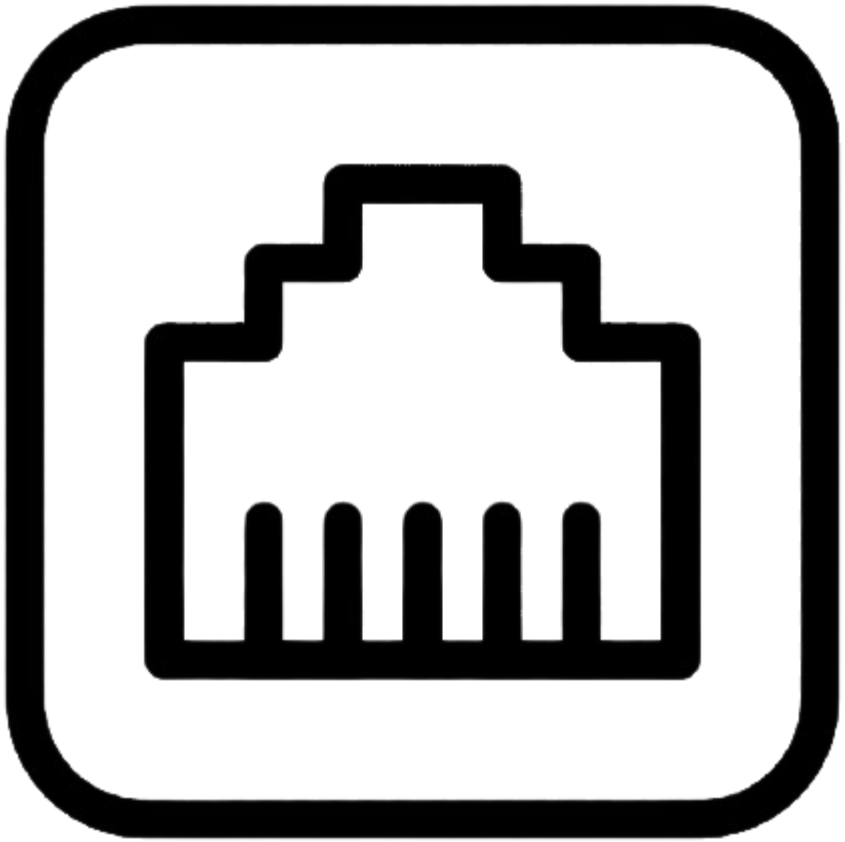
Pour vous connecter au serveur entrer l'adresse IP de la machine serveur sur Putty et son port et le tipe de connexion



Tentative de connexion à distance

Si vous entrer les logs de l'un de vos utilisateurs et le mot de passe vous êtes censé avoir ceci :





CHANGEMENT DE PORT

Tentative de changement de port

Il est important de changer le port de votre SSH en effet car le port 22 automatiquement saisi lors de l'installation de votre système d'exploitation,
Il est aussi important de changer le port pour éviter les attaques brutes force ou de l'homme du milieu

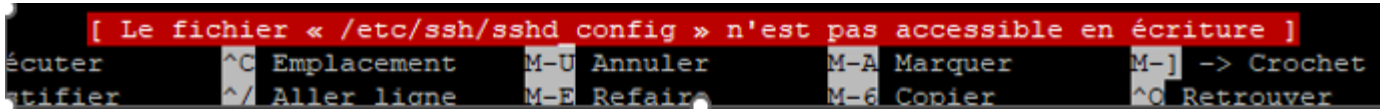
Attaque brute force: méthode utilisée en cryptanalyse pour trouver un mot de passe ou une clé. Il s'agit de tester, une à une, toutes les combinaisons possibles

Attaque homme du milieu: attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre puisse se douter que le canal de communication entre elles a été compromis.

Tentative de changement de port

Pour changer le port de votre serveur vous devez aller dans le fichier nano /etc/ssh/sshd_config

ATTENTION: il est important de modifier ce ficher en tant que root et pas utilisateur car sinon vous n'aurez pas les droits d'écriture pour modifier le fichier :

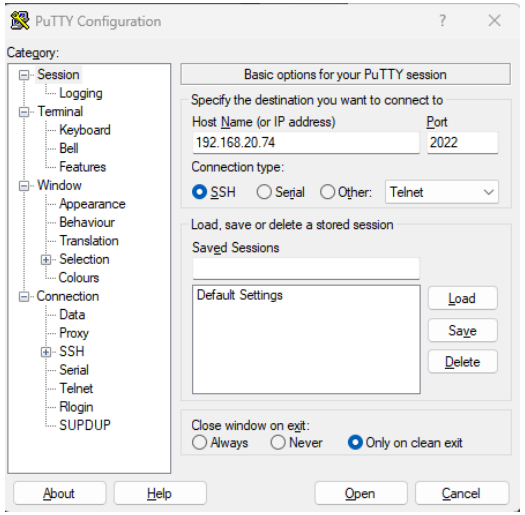


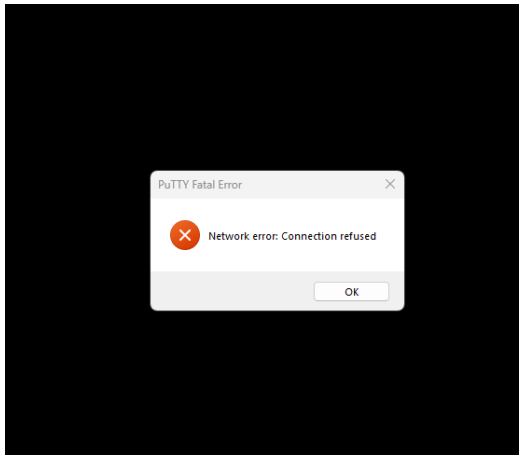
Pour modifier le port d'entrée décommenter la ligne et inscrivez-y le port 2022

Redémarrer le service avec la *commande service ssh restart*

Tentative de changement de port

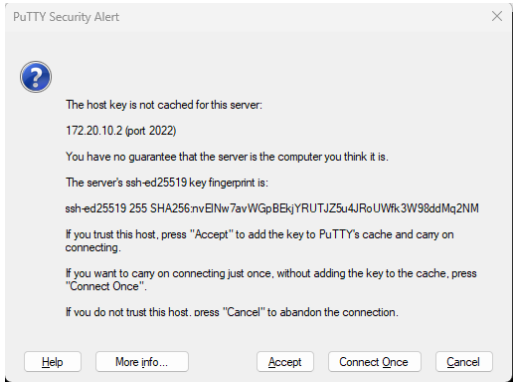
Essayer de vous reconnecter avec votre machine cliente sur le serveur et vous pouvez observer qu'il y a une erreur.
Ceci peut être du fait que le pare-feu n'autorise pas le trafic sur le port 2022 activez l'autorisation avec la commade ufw allow 2022





Tentative de changement de port

Ceci est tout à fait normal que la connexion à votre serveur SSH ne s'effectue pas car le pare-feu bloque l'accès.
Pour pouvoir vous connecter sur le port 2022 vous devez
-Installer ufw avec la commande apt install ufw
-Autoriser les connexions SSH sur le port 2022 avec la commande sudo ufw allow 2022
-Activer le UFW avec la commande ufw enable
-Relancer votre machine
-Connecter vous sur Putty en modifiant le port et vous pouvez voir qu'on peut maintenant se connecter sur le port 2022



(l'adresse IP n'est pas la même car j'ai essayé de rentrer grâce au port 2022 de mon côté)

CRÉATIONS ET ÉCHANGE DES CLÉS PUBLIQUES

Autorisation login root /Permettre les mots de passe vide

PermitRootLogin: Définit si oui ou non le super-utilisateur Root a l'autorisation de se connecter par ssh.

Dans l'idéal il serait judicieux de mettre cette option sur no sur la machine car en cas d'attaque de brute force le pirate aura un accès direct au plus au niveau du privilège de la machine et pourra faire tout ce qu'il souhaite

PermitEmptyPasswords Définit si le serveur accepte la connexion à un compte utilisateur ne possédant pas de mot de passe

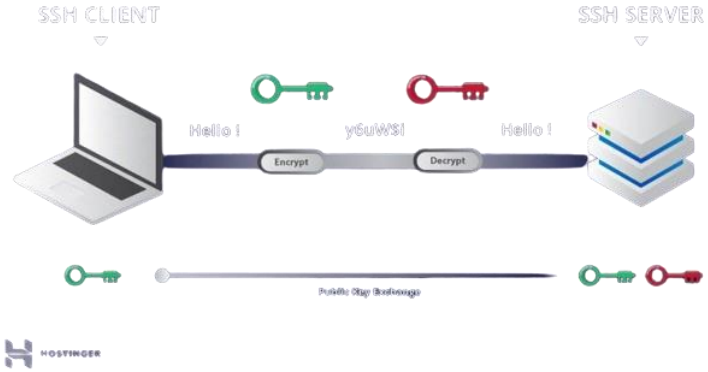
La différence entre ces deux machines est donc que "PermitEmptyPasswords" se concentre sur l'autorisation des connexions avec des mots de passe vides, tandis que "PermitRootLogin" contrôle l'accès en tant que superutilisateur (root) et peut spécifier si l'authentification doit se faire sans mot de passe

Gérer l’échange des clés publiques

Tout d’abord une clé SSH est un identifiant d’accès pour le protocole réseau SSH (Secure Shell).Ce protocole réseau sécurisé authentifié et chiffré est utilisé pour la communication à distance entre des machines sur un réseau ouvert non sécurisé.

Comment cela fonctionne ?

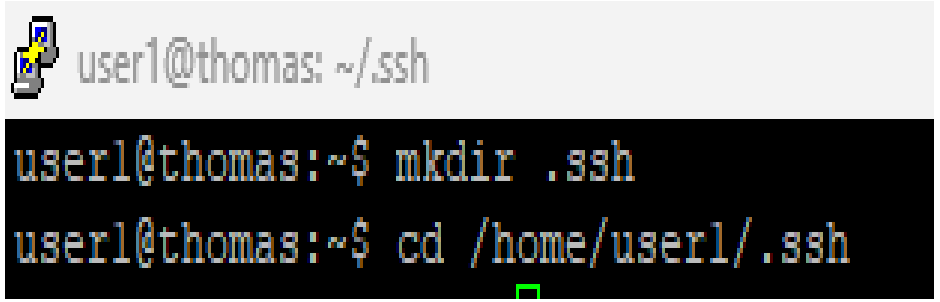
Le serveur distant utilise une clé publique pour chiffrer un message de défi aléatoire qui est renvoyé au client. Ce message de défi est déchiffré à l’aide de la clé privé de votre système

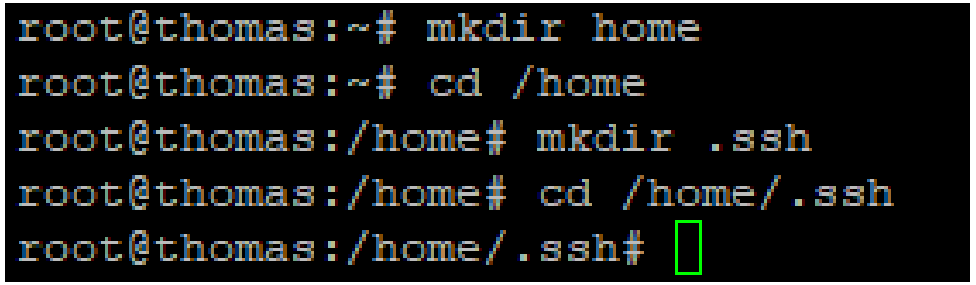


Gérer l'échange des clés publiques

Nous allons maintenant devoir créer des clés d'authentification pour pouvoir effectuer ceci on va devoir créer un répertoire .ssh pour chaque utilisateur pour pouvoir gêner nos clés dans ce dossier.

Pour créer ses dossiers connecter vous a chaque utilisateur et diriger vous dans le répertoire avec la *commande cd /home/nomuser*
Une fois dans ce dossier créer un dossier .ssh avec la *commande mkdir .ssh*
Pour l'utilisateur root il faut d'abord créer un dossier home puis ensuite un dossier .ssh





Gérer l'échange des clés publiques

Nous allons maintenant donner des droits d'accées au fichier avec la commande chmod 0770 /home/nomuser/.ssh pour chaque utilisateur

```
root@thomas:~# chmod 0770 /home/user1/.ssh
root@thomas:~# chmod 0770 /home/user2/.ssh
root@thomas:~# chmod 0770 /home/user3/.ssh
root@thomas:~# chmod 0770 /home/.ssh
```

Gérer l'échange des clés publiques

Maintenant il faut que vous générer vos clés publiques pour chaque utilisateur à l'aide de la *commande ssh-keygen -t dsa -f /home/nomuser/.ssh/id_dsa* . Entrer une passphrase en respectant les normes de complexité d'un mot de passe (12 caractères minium, caractères spéciaux, lettres , chiffres)

```
root@thomas:~# ssh-keygen -t dsa -f /home/user1/.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 /home/user1/.ssh/id_dsa
Your public key has been saved in /home/user1/.ssh/id_dsa.pub
The key fingerprint is:
SHA256:qMK7kkDASqzSVVjB2Bh7fx754UMQuSuBITcL9gl+Qdk root@thomas
The key's randomart image is:
+---[DSA 1024]----+
|o   .@=+  ..     |
|.+  X.O E ..     |
|=. +.*.B  ..     |
|+.. ..*o. .o     |
|o    .. S.+.o    |
|..   .  .o.= .   |
|..o .    .. +    |
|o  o         .   |
| .o.             |
+----[SHA256]-----+
```

Faites ceci pour chaque utilisateur

Gérer l'échange des clés publiques

Copier vos clés publiques vers votre serveur pour qu'il puisse vous identifier à l'aide la *commande ssh-copy-id -i ~/.ssh/id_dsa.pub root@adresseIPserveurSSH*, à la première connexion, on vous demande s'il faut accepter une empreinte. Il s'agit de la clé publique du serveur qui sera déposée dans le fichier des hôtes connus (~/.ssh/knownhosts)

```
root@thomas:/home/user1/.ssh# ssh-copy-id -i ~/.ssh/id_dsa.pub user1@192.168.0.23
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_dsa.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
user1@192.168.0.23's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'user1@192.168.0.23'"
and check to make sure that only the key(s) you wanted were added.

root@thomas:/home/user1/.ssh# ssh-copy-id -i ~/.ssh/id_dsa.pub user2@192.168.0.23
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_dsa.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
```

Gérer l'échange des clés publiques

Si vous vous demandez quelles clés se retrouvent dans le dossier authorized_keys il vous suffit d'ouvrir ses fichiers.
Déplacer vos dans le fichier .ssh a l'aide de la *commande cd /home/nomutilisateur/.ssh*

Faites un ls et vous pouvez qu'il y à différents fichiers.
Ouvrez le fichier known_hosts a l'aide la *commande cat known_hosts* dans ce fichier on peut retrouver la clé publique de tous les serveurs SSH sur laquelle ce compte s'est connecté

```
root@thomas:/home/user1/.ssh# cat known_hosts
|1|1gDhnHBcGjB5ARrZS0lp9ONaBK8=|lJWc3CahSRSJBLvS4aERv2Lg58c= ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAILO
a6IGQn8FlN0WKPfomdzSBL
|1|MxBam06NNSz7+H8s3uug/l/bNqg=|F/L7BP+IkjwUC88FcSJ/97qrZbM= ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC
5o0mcFiugaLQ8AUSYbLJSIa4b0T+xpWzCCA8AAe29MHAP/sSAMzoEPU4fnvEhFMqGhYn8W7KH96nN/CTdRng1z/6nJ61wnVrVsq9
rOF2Hfp1H9WlFc+axXZILz5WqGrE9IHqu21IzRkhIq1oZwvEDp9v7D4iDh56wQPaJmloLqGpOlUjVVRR2p2rQzQlPcproLG+nP4T
6idotBwvQeu/RSQpS9dR36fJ4MAj4bMzHAaE+nEN6ArtLzpetLVTpnsWxOFVwcd/ZbiW5vhMTKwjUS1zrIbMYtlOG40BFWzhiBzv
lHfZa8u5QPXL9W9swE5WaJTqACB3J6LfHKMOcYWcCeVSPSMRubM1MbFaBoDQNY3wb/GyEd8gBOrVnA+2iqXZcki16rUXEQHNRA/c
eLgmxK7l3gCbXAjAk=
|1|+DTQViluHT5Yy6lWLzE53sYqSsI=|WjYgcsoy1JO8yk9virG7wHAMSTU= ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTI
lzdHAyNTYAAABBBO9KFBjsh4mWLU9YsL4TPkeIOkpwCoM9s/28H4UwNZyqTq8vi/uwK8NnL3SOcpDiodMRE9jwgS2uYZmuoS5E6+
```

Gérer l'échange des clés publiques

Dans le fichier id_dsa on peut y retrouver la clé privé

```
user1@thomas:~/.ssh$ cat id_dsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1NiljdHIAAAAGYmNyeXB0AAAAGAAAABCJtRdDLY
fyNKr0fchWx4YGAAAAEAAAAAEAAAGxAAAAB3NzaC1kc3MAAACBALTmG5lgm3TLfqZ7BASw
yD2nmKUv4r7YP+ngk6Xp0dcgBnUpaSbhGSnxUClAnPP98rONgzAFKBbygGzEMmHaS5i3+H
jSDkCDqiPojDbqWCd7Q57KxpiASCda3NgdtcxFtI5S+aF5sZjdz8P9LKlGfR72H8qcPD0X
mrEH4w2mn4W3AAAAFQDhl9i48bcGBfukG0/xOm3nBYjMLQAAAIBE3tMfclK7PdY4vlx0gU
oU8J05lRN0OcQpAopfkf7plk/am4RfvWoZWR5UOLj++dXpZg00ATzlWWfvLx3jdxcOmlpX
/RsQVAPXmVlhhqII/TIioIoOtoOl4W3j/djIyA6gacd6H6p9fbbO8YK0kfcVllltvlKqWq
u3olt+WPctRAAAAIBYGnWrhDjjMsVimKNt6tNPkf7rMc8cjbgpF22TMbMFA/nVZBouRiUi
uCJ9f9uVA7nxxemyJuDUtrB7XjzESVQK3N+mVwflzsB/9de/wSvvU6vPTMaZeM3Cbu0s+N
jjjIzuQO6alfiCATrlGjZU+OWhJvtaSt9RLtNoU5HD4+lCNAAAAfAj+sJlexNzVri/BHa3
6ZbbfGZQNVEpkSx5bV7KclzRuknZuLP9qsJYs8zu5hJKvrUcGVTbbxF4pFnGG3q7ljN6Vx
3LizP95g3BbdFQbQJkPcgc4VUzHNSOQ+7QbeYawE3F0VB3W60Kc4pjGDOtdj0IWAjMYut0
GpcTdldvEqHk/OwCRA25mTy2bSl6jxnIcUP8nGtRHYu8Smp72PNPJvZvBytJmRuy8YAv2C
6nAGqgcMpTf7D4A5MnD8pjKwifULyNIZgqp3ctyYeLvLqZJRbBtzFRkODPllzAp4QQRBec
JbSo28cQgXUz8uO3dbjfeBs92tAdMi815pVSpnkkor0zkandKDjEep7qbEBhIHL6AuSA4u
KFPBNCtao96yKG84sxAmXytlq2qQWS/J1XKkQP2cqhfCDgUbkdKnC+ZSGl2BCFYTp7/aEN
hXmlgKsE8oHLQyYhqE7z0c6TgQunVswnbJ55WfrwRnVZCEcSlop4JLvC9chwF7Uf0Jui+u
lLwS3JAMEvKqR6zx5pPyjN4VSwn/Bgj0iyEVZq6CXBQtXCndFI2fIKix2Y+ZOkOV/v9aOH
PV8Cnn5WXmLaU7bBWrDhfQcGLbNqv5NT6fIgkPU3RwxXE9KigDBEbtRBAjTMxjg5bQ8dvf
iX3+l6obG+fOWx
-----END OPENSSH PRIVATE KEY-----
```

Gérer l'échange des clés publiques

Dans le fichier id_dsa.pub on peut y retrouver la clé publique qui sera ajouté au fichier authorized_keys

```
user1@thomas:~/.ssh$ cat id_dsa.pub
ssh-dss AAAAB3NzaC1kc3MAAACBALTmG5lgm3TLfqZ7BASwyD2nmKUv4r7YP+ngk6Xp0dcgBnUpaSbhGSnxUC1AnPP98rONgzAFKBbygGzEMmHaS5i3+HjSDkCDqiPojDbqWCd7Q57KxpiASCda3NgdtcxFtI5S+aF5sZjdz8P9LK1GfR72H8qcPD0XmrEH4w2mn4W3AAAAFQDhl9i48bcGBfukG0/xOm3nBYjMLQAAA
IBE3tMfc1K7PdY4vlx0gUoU8J051RN0OcQpAopfkf7p1k/am4RfvWoZWR5UOLj++dXpZg00ATz1WWfvLx3jdxcOmlpX/RsQVAPXmV1hhqII/TIioIoOtoOl4W3j/djIyA6gacd6H6p9fbbO8YK0kfcV111tvlKqWqu3olt+WPctRAAAAIBYGnWrhDjjMsVimKNt6tNPkf7rMc8cjbgpF22TMbMFA/nVZBouRiUiuCJ9f9
```

```
user1@thomas:~/.ssh$ cat authorized_keys
ssh-dss AAAAB3NzaC1kc3MAAACBANNl/GYVBrx7qBQ6eE2P+rh7ZRhLule1C5ul+zPUGNz+q0QLdJJkT8LPI5x3uUj9Cy9qqtMdBpXGEBa4vsEqlr2plZbj7neinAkdaoPKViyTVxivc69lSWD8B6+MlczpwplgYRUueb2yv9GuBIoZw/zGgSBYkeDiv+lxwQLbueIFAAAAFQCR0u2O6S8w3YxeRJJtJVNXMxz0xwAAA
IEAwRnfE/rmpUy4g8Zbc/R7oCwcw9MzANM/fBikwfX2/4kpvkXsyNGLl/Qphmrv90gSSD0LL3tzEfybzCP7FyNAvgsbq7DgjNi9UXsZlF7iUEIBBMtb6TwW3RBSOErd3iDQ+37FBkw9ZFMxON2qZ+wAJsyyIy5eHYdHOi9oMgplvn8AAACBAI5pNlvXfODqh9vsRZsGwdEL9lb3N/FEe3xL7Eki0BFWhoYhXLv8nI4n3p
vchWcXzQWL18RZ9TxgK0BKN8xHXLFx8mEX4aNRYiZJg22aRBNqXc418HHg7/zvJJzlO3GNw0ZQ0gon/PvqOJxLTzwfk6JPtvyqeE3uDlSodoUegxv5 user1@thomas
ssh-dss AAAAB3NzaC1kc3MAAACBAI694MMqQx7GjkH243GLwNDxFpkko7iaQABZBvxeEIA96lCD8wCWulmxpYkw08WkmKC2mCOOYmP/N8burulNEyZSXvsAxWivUUz/RTF8z54EKflJSB6lsZYfiX/uuRLVrkWL3iOVO8z5wShRXIb+kmVWP3OLht+2gTKKYbHkPa8fAAAAFQCRSyW5TtsiPxpsvfNiu+NUwyynmQAAA
IANGni50hK36vghqj7Gp2tfbB8ieFolQ2Un+bvxte8xcgyV/K8MmET5aXt29BpC0U20Gtl E4qPvnY2d7NF64GHTyyhBYFlmKlXwS9kw4C9DPwZ/sH9d73UltWgeI4ZwzRMdnpkdOsul9QZW4czDHlzbIB4Kkg1lwtVdqMM4OjOrEQAAAIBHOHy9NiPdmeyOSAPs762kLZSJ3hl4otj/7MtjO5OHUd0v8RHxAsYezEL7Ns
2FwGlCTJ/8n2VHMksWzqzhykJOJVdRowBR2khWX3wlvltMI6u9GTWaGlYb2csoOnIgPxQYQT3DfY2siw2HlgdqPlJ2DZ+O/eLG7AbF+S3Xj9eqvw== root@thomas
ssh-dss AAAAB3NzaC1kc3MAAACBAImlzp/+BSKtywVvql6FbTIO8bmXPm2mC3GF9MrW2gQxHtqyyJi6PAMIF0LltrSaIOv8IX0jx9sxZoaNdlrjG6JImluVWT0jqXrwUEedNKY2WNtgjAdlRmozwlgilwSTTxWGmEmA1rH0yTdlRxL33yhrjILDq9rzynBQc/agRg7PAAAAFQDsmP3yl5JrKo46oLVFo+3Dup7YMwAAA
IA6z0hQRraX6hXS6JlrCgbYr/WgdzyGpoCnaLkSh19O6EARY/KTfJLAb5jpRYKlnOb7ifndIV5XYMk4nk29iekA+DbZy59L7mGjV4Lq0J84c0d6yHK7vD5dBbXb9fkgrKmEeJ5vn7WNQTREtUzleeaJZfggWQqhv/9Y27I/ff0ieAAAAIBmtAFXy/5d4lFYrfLPT+HLml4ArUS2WUVAEA/CThLtrFCgoPJTG70VG+1Fia
FMMjOA0nLeneUITk+4ZLuBhwiskjsaeeGSKb8HV7lqlIXMyJdWNUvCaeIDkzjBLvrncXZRGx3YzQohYw+zXHlxdvO3/lezgWulNUrwd47lyk8c0w== root@thomas
```

La clé publique se retrouve dans le fichier authorized_keys car lorsque un utilisateur souhaite se connecter au serveur SSH, le serveur vérifie la clé publique fournie par l'utilisateur avec celles présentes dans le fichier authorized_keys.
Si une correspondance est trouvé, l'utilisateur est autorisé à se connecter sans à fournir un mot de passe

Tester la connexion au serveur SSH

Nous allons maintenant tester notre connexion au serveur SSH

Pour vous connecter au serveur SSH à distance il suffit *d'entrer la commande ssh nomuser@adresseIP –p port*

```
user2@thomas:~$ ssh user3@192.168.0.23 -p 22
user3@192.168.0.23's password:
Linux thomas 6.1.0-17-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.69-1 (2023-12-30) 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.
```

Pour savoir qui s'est connecté à votre serveur SSH il vous suffit de rentrer la *commande who* sur votre serveur et vous aurez l'heure et utilisateur connecter à votre serveur SSH

```
root@thomas:/home/thomasg# who
thomasg  tty1         2024-02-07 17:21
thomasg  pts/0        2024-02-07 19:17 (192.168.0.50)
user1    pts/1        2024-02-07 20:19 (192.168.0.50)
user1    pts/2        2024-02-07 20:31 (192.168.0.23)
user1    pts/3        2024-02-07 20:33 (192.168.0.23)
user1    pts/4        2024-02-07 20:34 (192.168.0.23)
user2    pts/5        2024-02-07 20:35 (192.168.0.23)
user3    pts/6        2024-02-07 20:38 (192.168.0.23)
```

Tester la connexion au serveur SSH

Si vous voulez limiter la connexion de certains utilisateurs sur le serveur SSH, vous devez modifier le fichier de configuration sshd_config et ajouter la ligne AllowGroups + nomgroupe ou alors Allowusers + nom users `AllowGroups ssh root`

Quand on essaye de se connecter avec le user3 on aura donc bien un accès refusé car il n'est pas autorisé de se connecter au serveur SSH

```
login as: user3
user3@172.20.10.2's password:
Access denied
user3@172.20.10.2's password:
```

Alors que le user1/2 sera autorisé

```
login as: user1
user1@172.20.10.2's password:
Linux thomas 6.1.0-17-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.69-1 (2023-12-30)
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 15:20:57 2024
```

Connexion avec la clé d’authentification

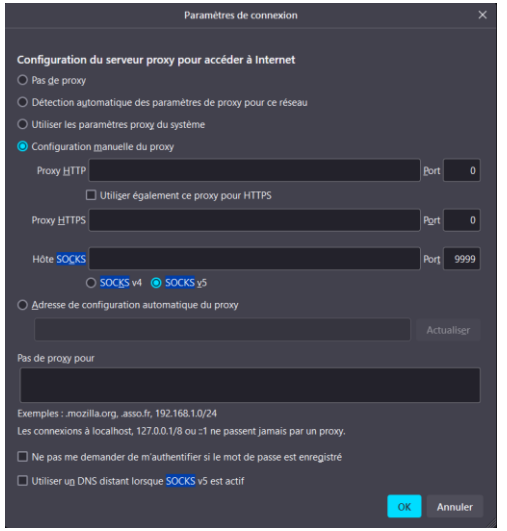
Pour vous connecter avec la clé d’authentification vous devez modifier le fichier sshd et basculer la ligne de commande PasswordAuthentication yes en no.Cette ligne permet de se connecter au serveur SSH avec un mot de passe ou alors avec la clé en no

Il se peut que cette ligne de commande « bug » et j’ai ce bug après de multiple de recherche sur internet j’ai trouvé aucune solution et c’est bien une erreur qui vient du serveur SSH

Les plus du TP SSH

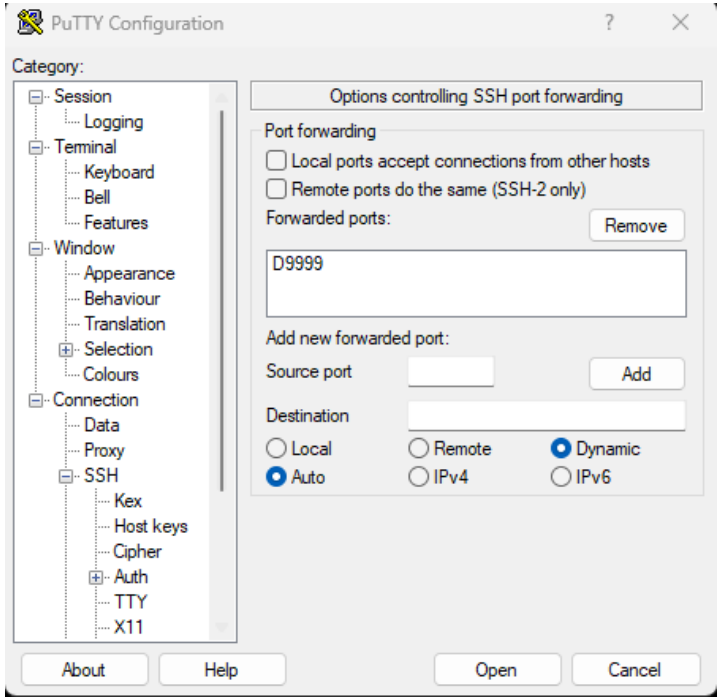
La partie qui va suivre à était commencé mais pas fini à cause d'un souci avec ma VM

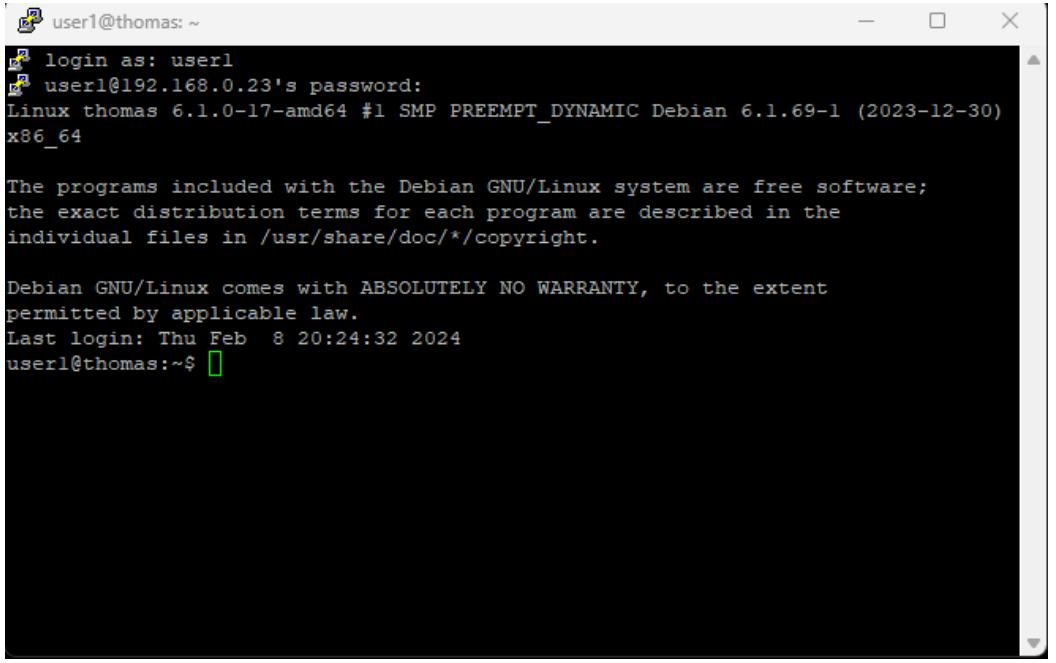
Nous allons maintenant utiliser le protocole SOCKS qui utilisé comme pare-feu réseau
Pour faire ceci aller sur Firefox puis dans les paramètres proxy
Entrer le port 9999 pour faire un changement d'adresse et de port



Les plus du TP

Sur Putty allez dans SSH -> tunnels et ajoutez le port 9999 en dynamic et auto effectuer ensuite une connexion SSH et connecter vous sur votre serveur SSH





Les plus du TP

Maintenant lancer un Wireshark sur votre machine et lancer une page internet et connectée vous sur http://google.fr (Il manque un screen a cause d'un problème avec ma vm)