

Département Informatique

R 2.05 – TP SSH

Responsable : X.Roirand

Durée : 90mn machine

Le but de ce TP va être d'utiliser ssh et d'installer un serveur ssh sur une machine, de le faire fonctionner avec des configurations qui sont demandées. Il y a beaucoup de questions et vous ne répondrez peut-être pas aux dernières par manque de temps, pas grave, considérez ces dernières questions comme des questions « bonus ».

Document de rendu :

Créez un document qui va contenir les réponses que vous allez donner au fur et à mesure de l'avancement dans le TP (ce document sera à rendre dans la zone de rendu « TP SSH » sur Moodle dans l'UE R 2.05).

Toutes les questions auxquelles vous devez répondre dans le document de rendu sont de la forme :

Question x) cherchez comment ...

1) Utilisation de ssh

SSH est un protocole permettant de se connecter à un ordinateur distant. A la différence d'autres protocoles non sécurisés comme Telnet ou rlogin qui véhiculent l'information en clair, SSH nécessite une authentification mutuelle du client et du serveur et les données sont chiffrées.

L'authentification se fait par mot de passe ou par clé publique.

SSH est présent nativement sous les systèmes Unix et MacOS. Sous Windows, il existe plusieurs utilitaires pour vous permettre de vous connecter en SSH (par ex : putty).

Utilisation :

(Mac/Linux/Windows WSL) :

```
ssh login@machine_distante
```

ou

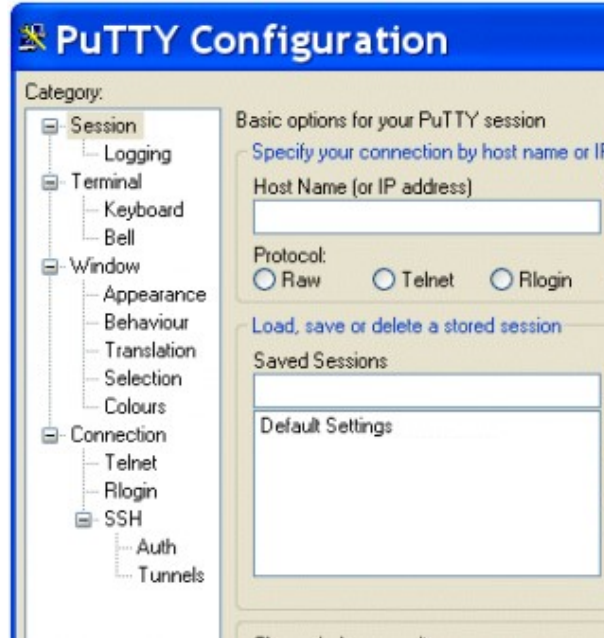
```
ssh machine_distante -l login
```

(Windows) :

Putty est un petit utilitaire qui permet de faire des connexions SSH sous Windows.

Téléchargez putty.exe à cette adresse :

<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>



Il s'agit d'un exécutable, pas besoin d'installation. Placez le fichier à l'endroit qui vous convient et lancez le.

Voici les différentes informations nécessaires pour faire fonctionner une connexion ssh sous Putty :

- host Name (or IP Address) : Indiquez l'adresse IP ou le nom complètement qualifié du serveur que vous voulez contacter
 - Protocol : Cochez SSH
 - Cliquez sur Open.
 - A l'invite de commande, entrez votre login et votre mot de passe.
- Nota* : Il est possible d'enregistrer vos diverses sessions.

2) Connection sur la machine distante

Vous aller commencer par vous connecter sur une machine distante appelée « Sandbox », qui est un point d'entrée sur l'ensemble des machines du réseau mis à disposition des étudiants pour ces TP. Une fois connecté sur cette sandbox, vous pourrez ensuite vous connectez sur votre machine finale sur laquelle faire le TP. Cette double étape sera à répéter à chaque TP, pensez-donc bien à la noter, afin de gagner du temps pour les prochains TP.

Pour se connecter sur la sandbox, vous avez besoin d'un client ssh (voir début de ce TP) d'une adresse ip (celle de la sandbox), d'un utilisateur et d'un mot de passe, voici ces informations :

Ip : 198.27.82.182
 User : student
 Mdp : ?Student_56

Une fois sur cette sandbox, connectez-vous sur votre machine distante finale, pour cela vous aller utiliser un client telnet et l'adresse ip de votre machine finale.

Question 2) D'ailleurs, quel est la différence entre telnet et ssh ? Répondez à cette question en quelques lignes dans votre document de rendu (il vous faudra probablement chercher sur internet).

Pour se connecter en telnet depuis la sandbox, il faut connaître le numéro que le professeur vous a donné, et utiliser telnet comme suit :

telnet 192.168.0.X ou X est votre numéro

Exemple : si votre numéro est le 23 alors il faut faire :

telnet 192.168.0.23

Ensuite le login et mot de passe sur votre machine distante sont :

login : student

mot de passe : ?<votre numéro>Student_56

Exemple : si votre numéro est le 13 alors il faut faire un ssh sur la machine ssh3

login : student

mot de passe : ?13Student_56

Une fois sur votre machine distante finale, vous pouvez l'administrer totalement car le user student sur cette machine peut faire des commandes sudo.

ATTENTION : la 1^{ère} fois que vous vous connectez sur votre machine finale, changez votre mot de passe de l'utilisateur student. Si vous ne le faites pas, toute personne connaissant votre numéro pourrait se connecter en tant que student sur votre machine finale et en faire ce qu'elle veut !!!

Question 3) Cherchez sur internet à quoi sert la commande sudo et expliquez le dans le document de rendu.

3) Installation du serveur SSH sur votre machine (finale)

Installer maintenant le serveur SSH sur votre machine finale (celle mis à disposition par l'enseignant). Pour cela il faut d'abord trouver un package (ensemble de fichiers permettant d'ajouter une fonctionnalité sur le système) qui contient un serveur SSH. Pour cela il existe une commande sur toutes les distributions Linux moderne qui permet de faire cette recherche et d'affiner les résultats.

Chercher sur internet comment chercher un package qui contient un nom donné pour Ubuntu (la distribution Linux de votre machine finale).

Question 4) Indiquez dans le document de rendu quelle commande vous avez utilisée pour rechercher et trouver le package du serveur ssh à installer.

Chercher sur internet comment installer le package que vous avez trouvé. N'hésitez pas à demander à votre enseignant si vous ne trouvez pas ou si vous avez un doute sur le nom du package.

Question 5) Indiquez dans le document de rendu quelle commande vous avez utilisée pour installer le package du serveur ssh.

Une fois le serveur installé, lancez le (cherchez sur internet comment lancer un service sous

Ubuntu).

Question 6) Indiquez dans le document de rendu quelle commande vous avez utilisée pour lancer le serveur ssh. Il existe plusieurs manières de le lancer, prenez la plus récente.

Une fois le serveur lancé, vérifiez qu'ils s'est bien lancé (cherchez sur internet comment vérifier le status d'un service sous Ubuntu).

Question 7) Indiquez dans le document de rendu quelle commande vous avez utilisée pour voir le status du serveur ssh.

Bon, maintenant que le serveur ssh est installé sur votre machine finale, il faut le tester pour voir si ça marche. Pour cela, connectez vous sur la sandbox et ensuite faite une connexion vers votre machine finale, non pas avec telnet cette fois ci, mais avec le client ssh, avec la même syntaxe que dans le 1).

La première fois que vous vous connectez à une machine, un message comme ci-dessous apparaît :

```
The authenticity of host 'machine_distante (194.254.199.xx)' can't be
established.
RSA key fingerprint is 66:c7:c2:e5:2d:f5:5e:07:f6:95:d2:86:60:7c:ba:b8.
Are you sure you want to continue connecting (yes/no)?
```

Cela s'explique car à chaque connexion à un serveur, le serveur sur lequel vous vous connectez vous donne sa clé publique et vous (enfin plutôt le client ssh que vous utilisez) l'enregistrez dans un fichier. Normalement, la toute première fois qu'une machine est installée, elle génère sa paire de clé publique/privée et n'en change jamais plus. Cet enregistrement de votre client ssh, permet donc de stocker la clé publique envoyée par le serveur et pour les connexions suivantes, de comparer celle qui est envoyée par le serveur avec celle qui a été stockée lors des connexions précédentes. Si jamais il y a une différence, ce qui ne doit quasi jamais arriver, alors vous aurez un warning car cela signifie probablement que vous ne vous connectez pas sur la machine que vous croyez mais sur une autre.

Question 8) Indiquez dans le document de rendu quelle commande vous avez utilisée pour tester le serveur ssh depuis la sandbox avec le client ssh.

Question 8bis) cherchez le fichier dans lequel est stocké la clé publique du serveur sur lequel vous venez de vous connecter (il faut donc réussir la connexion avant de chercher).

Indiquer dans votre document de rendu, le nom du fichier et mettez aussi son contenu

4) Configuration du serveur SSH

Changer maintenant le port d'écoute du port ssh, trouvez le port par défaut et le changer par le port 2222. Pour cela chercher sur internet où est le fichier de configuration du serveur ssh. Attention, il y a un fichier de configuration pour le client et un pour le serveur, ne vous trompez pas.

Question 9) Indiquez dans le document de rendu quelle ligne (ancienne ligne et nouvelle ligne) vous avez modifié et le nom du fichier de configuration. Indiquez aussi quel était l'ancien port d'écoute, celui par défaut. Si vous ne le retrouvez plus, cherchez sur internet.

Ajouter l'utilisateur student2 sur la machine finale. Chercher sur internet comment rajouter un utilisateur. Attention il faut penser à trouver la commande qui par défaut crée le répertoire de base du nouvel utilisateur ou utiliser une option d'une commande qui permet de créer ce répertoire de base (home de l'utilisateur).

Question 10) Indiquez dans le document de rendu la commande que vous avez tapé pour créer ce nouvel utilisateur.

Question 11) Quelle commande pourriez vous faire pour afficher le contenu de la home cet utilisateur student2 ?

Vous avez créé l'utilisateur mais...comment vérifier qu'il est fonctionnel ? Simple, connectez vous sur la sandbox et ensuite faites un ssh sur votre machine finale en tant que student2, normalement cela devrait fonctionner.

Question 12) Indiquez la commande que vous avez tapé pour vérifier le fait que l'utilisateur student2 puisse se connecter sur votre machine finale ?

Trouvez maintenant comment empêcher que l'utilisateur root puisse se connecter via ssh sur votre machine finale et testez que cela fonctionne. Testez que par contre on peut toujours se connecter en tant que student sur la machine finale.

Question 13) Indiquez la ligne que vous avez modifiée ou retiré ou ajouté dans le fichier de configuration du serveur ssh pour interdire la connexion ssh en tant que root ?

5) Connection ssh de la sandbox vers votre machine finale sans mot de passe avec une passphrase vide :

Essayer de trouver sur internet comment se connecter de la sandbox à votre machine finale en ssh sans saisir de mot de passe avec une passphrase vide, tout cela avec l'utilisateur student.

Question 14) Indiquez ce que vous avez dû faire pour que tout fonctionne comme demandé ?

6) Connection ssh de la sandbox vers votre machine finale sans mot de passe avec une passphrase non-vide avec une clé de 4096 bits:

L'exercice est comme celui de la question précédente sauf que les clés générées par défaut et qui sont sous /home/student/.ssh contiennent une passphrase vide, il faut donc que vous créiez votre propre paire de clés, que vous ne pourrez stocker que sous /tmp. Créer cette paire de clé, avec une passphrase non vide et utiliser cette paire de clé pour se connecter depuis la sandbox vers votre machine finale, en tant que le user student sur les 2.

Question 15) Indiquez ce que vous avez dû faire pour que tout fonctionne comme demandé ?