Partie I: Première utilisation de SSH

Notes :

* Les commandes précédées de "$" signifient que vous devez exécuter la commande en tant qu'utilisateur général - et non en tant qu'utilisateur root.
* Les commandes précédées de "#" signifient que vous devez travailler en tant qu'utilisateur root.
* Les commandes comportant des lignes de commande plus spécifiques (par exemple "rtrX>" ou "mysql>") signifient que vous exécutez des commandes sur des équipements à distance, ou dans un autre programme.
* Si une ligne de commande se termine par "\", ceci signifie que la commande se poursuit sur la ligne suivante et que vous devez la traiter comme une seule ligne.

1. Connectez-vous à votre PC en SSH

Utilisateurs Windows

Si vous utilisez Windows et ne disposez pas d'un client SSH, vous pouvez télécharger une copie du programme SSH libre Putty à l'adresse suivante :

https://nsrc.org/workshops/2016/afnog-nmf/

Cliquez droit et enregistrez le fichier putty.exe sur votre Bureau ou à tout autre emplacement où vous stockez vos logiciels. Une fois enregistré, double-cliquez sur l'icône putty. Pour vous connecter à votre PC, saisissez le nom du PC dans la boîte "Host Name (or IP address)" (nom d'hôte ou adresse IP)dans putty :

pcN.ws.nsrc.org

Putty vous retournera alors une alerte de sécurité vous indiquant que la clé hôte du serveur n'est pas déjà mise en cache sur votre machine. Cliquez sur "Yes" pour accepter la clé.

Au message d'invite "Login as" (se connecter en tant que) répondez "sysadm".

En réponse à la demande de mot de passe, saisissez le mot de passe donné en classe.

Cela devrait suffire. Vous êtes maintenant connecté à une session terminal sur votre machine. Pour vous déconnecter, tapez :

"exit"

ce qui mettra fin à votre session terminal.

Utilisateurs Unix/Linux/Mac OS X

Ouvrez une fenêtre de terminal sur votre machine. Si vous ne savez pas comment faire, demandez de l'aide à votre formateur.

À l'invite, tapez :

        ssh sysadm@pcN.ws.nsrc.org

Lorsque vous voyez s'afficher à l'écran un message d'avertissement semblable à celui-ci :

The authenticity of host 'pc12.ws.nsrc.org (10.10.4.12)' can't be established.
RSA key fingerprint is 73:f3:f0:e8:78:ab:49:1c:d9:5d:49:01:a4:e1:2a:83.
Are you sure you want to continue connecting (yes/no)?
(L'authenticité de l'hôte 'pc12.ws.nsrc.org (10.10.4.12)' ne peut être établie. L'empreinte de la clé RSA est 73:f3:f0:e8:78:ab:49:1c:d9:5d:49:01:a4:e1:2a:83. Voulez-vous vraiment vous connecter (oui/non)?

        Tapez "yes" et appuyez sur ENTRÉE.

Au message d'invite "sysadm@pcN.ws.nsrc.org's password:" Entrez le mot de passe donné en classe.

Cela devrait suffire. Vous êtes maintenant connecté à une session terminal sur votre machine. Pour vous déconnecter, tapez :

        "exit"

ce qui mettra fin à votre session terminal.

Partie II: Utilisée avancée de SSH
==========

1. Clients Windows
Connectez-vous à votre PC en SSH

1.1. Générez la paire de clés ssh publique/privée

Clients Windows
Double cliquez sur puttygen.exe

Sous "Parametres":

S’assurez que l type de clés à générer est "SSH-2 RSA"

Nombre de bit: 2048
Cliquez sur "Generate". Déplacez la souris, travaillez un peu jusqu'à ce que la barre de progression atteigne'o100%

```
    Key comment:        [Votre nom <your@email.address>   ]
    Key passphrase:     [choisir une passphrase            ]
    Confirm passphrase: [confirmez la passphrase           ]
```

Cliquez sur « Sauvez la clé publique ».
Donnez un nom "id_rsa.pub"
(SVP sauvegardez les fichiers dans le même répertoire que les executables)

Cliquez sur "Sauvez la clé privée » . Donnez un nom "id_rsa.ppk"

Sélectionnez le contenu de la clé publique pour le copier dans le fichier authorized_keys de OpenSSH

Quittez puttygen.

1.2 Copiez votre clé publique dans votre PC

1.2.1 Copier-coller votre clé

Connectez vous vous à votre PC avec le compte 'sysadm'

```
$ cat >>.ssh/authorized_keys
    *** Collez la clé ***
    *** Si le curseur est à la ligne, appuyez sur Entrez ***
    *** Appuyez sur ctrl-D ***
```

1.3 connectez vous en utilisant votre clé privée

Démarrez putty. Entrez le nom de votre PC, mais avant d'ouvrir, allez sur Connection > SSH > Auth

```
    [-] Connection
         |
        [-] SSH
         |  |- Keyex
         |  |- Auth    <--- cliquez ici
```

A coté de « Clé privée ", cliquez pour chercher votre fichier id_rsa.ppk, ouvrez le, ensuite Ouvrir pour démarrer la connexion.

Qu'est ce que vous constatez??

1.4 Répétez la même opération pour d'autres PC ou serveurs

2 Environnement Linux (or BSD or OSX)

2.1 Générez une paire de clé publique et privée SSH

```
$ ssh-keygen -t rsa -b 2048
Generating public/private rsa key pair.
Enter file in which to save the key (/home/sysadm/.ssh/id_rsa): <HIT
ENTER>
Created directory '/home/sysadm/.ssh'.
Enter passphrase (empty for no passphrase): <CHOOSE PASSPHRASE>
Enter same passphrase again: <SAME PASSPHRASE>
Your identification has been saved in /home/sysadm/.ssh/id_rsa.
Your public key has been saved in /home/sysadm/.ssh/id_rsa.pub.
The key fingerprint is:
32:2b:e3:0e:14:fb:60:38:a6:e2:73:95:53:9d:a8:0f
sysadm@pcN.ws.nsrc.org
```

La passphrase est utilisée pour garder votre clé privée cryptée sur le disque.
Il peut être aussi simple que possible, ou aussi longue que vous voulez
Attention: si vous oubliez votre passphrase devient caduque.
On peut manger la passphrase en utilisant ssh-keygen -p

2.2 Copy votre clé publique dans le serveur

La méthode la plus simple est d'utiliser scp

```
$ scp .ssh/id_rsa.pub sysadm@pcN.ws.nsrc.org:.ssh/authorized_keys
```

Notez que .ssh/authorized_keys peut contenir plusieurs clés keys, une par ligne,

```
$ cat .ssh/id_rsa.pub | ssh sysadm@pcN.ws.nsrc.org 'cat >>.ssh/
authorized_keys'
```

2.3 connectez vous en utilisant votre clé privée

Connectez vous à votre PC

```
$ ssh sysadm@pcN.ws.nsrc.org
```

Que remarquez vous?
2.4 Répétez la même opération pour d'autres PC ou serveurs