

DOC : SHELL

Job 01

- Afficher le manuel de la commande ls

`man ls`

- Afficher les fichiers cachés du home de votre utilisateur

`ls -a /home`

- Afficher les fichiers cachés + informations sur les droits sous forme de liste

`ls -a -lisa <répertoire>`

- Comment ajouter des options à une commande ?

Avec des flags : `<commande> <flag>`

- Quelles sont les deux syntaxes principales d'écriture des options pour une commande ?

- flag (forme abrégée)
- flag (forme complète)

Job 02

- Lisez un fichier en utilisant une commande qui permet seulement de lire

`cat <nom du fichier>`

- Afficher les 10 premières lignes du fichier ".bashrc"

`head .bashrc`

- Afficher les 10 dernières lignes du fichier ".bashrc"

`tail .bashrc`

- Afficher les 20 premières lignes du fichier ".bashrc"

`head -n 20 .bashrc`

- Afficher les 20 dernières lignes du fichier ".bashrc"

`tail -n 20 .bashrc`

Job 03

- Installer le paquet "cmatrix"

```
sudo apt-get install cmatrix
```

- Lancer le paquet que vous venez d'installer

```
cmatrix
```

- Mettre à jour son gestionnaire de paquets

```
sudo apt update
```

- Mettre à jour ses différents logiciels

```
sudo apt update <logiciel>
```

- Télécharger+installer Google Chrome :

```
wget https://dl.google.com/linux/direct/google-chrome-stable_current_amd64.deb  
sudo dpkg -i google-chrome-stable_current_amd64.deb
```

- Redémarrer votre machine

```
/usr/sbin/shutdown -r now  
reboot
```

- Éteindre votre machine

```
/usr/sbin/shutdown now
```

Job 04

- Créer un groupe appelé "Plateformeurs"

```
sudo groupadd Plateformeurs
```

- Créer un utilisateur appelé "User1"

```
sudo useradd User1
```

- Créer un utilisateur appelé "User2"

```
sudo useradd User2
```

- Ajouter "User2" au groupe "Plateformeurs"

```
sudo usermod -g Plateformeurs User1
```

- Copier votre "users.txt" dans un fichier "droits.txt"

```
cp users.txt droits.txt
```

- Copier votre "users.txt" dans un fichier "groupes.txt"

```
cp users.txt groupes.txt
```

- Changer le propriétaire du fichier "droits.txt" pour mettre "User1"

```
sudo chown User1 droits.txt
```

- Changer les droits du fichier "droits.txt" pour que "User2" ai accès seulement en lecture

```
chmod o+r droits.txt
```

- Changer les droits du fichier "groupes.txt" pour que les utilisateurs puissent accéder au fichier en lecture uniquement

```
chmod a+r groupes.txt
```

- Changer les droits du fichier pour que le groupe "Plateformeurs" puissent y accéder en lecture/écriture.

```
chmod g+w groupes.txt  
sudo chgroup Plateformeurs groupes.txt  
setfacl -m g:plateformeurs:rw- groupes.txt
```

Job 05

- Ajouter un alias qui permettra de lancer la commande "ls -la" en tapant "la"

```
alias la='ls -la'
```

- Ajouter un alias qui permettra de lancer la commande "apt-get update" en tapant "update"

```
alias update='sudo apt-get update'
```

- Ajouter un alias qui permettra de lancer la commande "apt-get upgrade" en tapant "upgrade"

```
alias upgrade='sudo apt-get upgrade'
```

- Ajouter une variable d'environnement qui se nommera "USER" et qui sera égale à votre nom d'utilisateur

```
export USER=remi
```

- Mettre à jour les modifications de votre bashrc dans votre shell actuel

```
exec bash  
source .bashrc
```

- Afficher les variables d'environnement

```
printenv
```

- Ajouter à votre Path le chemin "/home/'votre utilisateur'/Bureau"

```
export PATH=$PATH:home/remi/Bureau
```

Job 06

- Vous devez télécharger l'archive suivante et la décompresser seulement avec le terminal.

```
tar -xzf Ghost\ in\ the\ Shell.tar.gz
```

Job 07

- Créer un fichier "une_commande.txt" avec le texte suivant "Je suis votre fichier texte"

```
ctouch une_commande.txt ; echo 'Je suis votre fichier texte' > a.txt
```

- Compter le nombre de lignes présentes dans votre fichier de source apt et les enregistrer dans un fichier nommé "nb_lignes.txt"

```
cd /etc/apt/ ; sudo wc -l sources.list > nb_lignes.txt
```

- Afficher le contenu du fichier source apt et l'enregistrer dans un autre fichier appelé "save_sources"

```
echo "$(<sources.list )" ; cp sources.list save_sources.txt
```

- Faites une recherche des fichiers commençant par “.” tout en cherchant le mot alias qui sera utilisé depuis un fichier

```
touch une_commande.txt ; echo 'je suis votre fichier texte' > une_commande.txt ; cd /etc/apt/ ; sudo wc -l sources.list > nb_lignes.txt ; echo "$(<sources.list )" ; cp sources.list save_sources.txt ; grep -r 'alias' .
```

Pour aller plus loin

- Installer la commande tree

```
sudo apt-get install tree
```

- Lancer la commande tree en arrière-plan qui aura pour but d’afficher toute l'arborescence en de votre / en enregistrant le résultat dans un fichier “tree.save”

```
tree ./ > tree.save
```

- Lister les éléments présents dans le dossier courant est utilisé directement le résultat de votre première commande pour compter le nombre d’éléments trouvés

```
Ls  
wc tree.save
```

- Lancer une commande pour update vos paquets, si l’update réussit alors, vous devrez lancer une upgrade de vos paquets. Si l’update échoue, votre upgrade ne se lancera pas

```
apt-get update  
apt-get upgrade
```

- Installer SSH

```
sudo apt install openssh-server  
sudo apt install openssh-client
```

- Générer une clé SSH

```
ssh-keygen
```

- Se connecter à une VM ou l'ordinateur d'un camarade via SSH

```
ip addr
sudo systemctl enable ssh      sudo systemctl enable ssh
systemctl start ssh
                                ssh remi@<adresse ip> -p <port>
exit
systemctl stop ssh
```

- Configurer SSH pour empêcher le login root (root ne peut pas se connecter en SSH)

```
sudo nano /etc/ssh/sshd_config
PermitRootLogin no
```

- Modifier le port de connexion de SSH (autre que 22)

```
sudo nano /etc/ssh/sshd_config
Port <port>
```

- Ensuite se connecter en SSH sans avoir à renseigner de mot de passe

```
ssh-copy-id -i ~/.ssh/id_rsa.pub remi@<adresse ip>
```

- Uploader un fichier avec SSH (de votre pc ou VM vers le pc ou VM d'un camarade)

```
scp <filepathoriginal> id@ip:<filepathdestination>
```

- Télécharger un fichier avec SSH (de votre pc ou VM vers le pc ou VM d'un camarade)

```
scp <filepathdestination> id@ip:<filepathoriginal>
```

- Limiter l'utilisation de SSH à un groupe particulier nommé "Plateforme_ssh"

```
chmod o-rwx /bin/ssh
sudo chown :Plateforme_ssh /bin/ssh
```

- Quel est l'intérêt d'utiliser SSH ?

SSH est un protocole sécurisé (beaucoup de paramètres de contrôle d'accès, gestion des droits user/groups).
Pas de login mais une clé d'authentification.

- Est-ce que les clés générées par SSH par défaut sont assez sécurisées ?

Les données sont cryptées par une key complexe (donc sécurisée), toutefois la clé privée doit être stockée sur l'appareil sur lequel vous vous connectez.

- Citez d'autres protocoles de transfert ? Quelles sont les différences entre ses protocoles ?

HTTP et HTTPS : HTTPS (Hyper Text Transfer Protocol Secure) est la version sécurisée de HTTP et permet un cryptage des communications via TLS ou SSL.

FTP : Premier protocole de transfert de fichiers, FTP est une méthode populaire de transfert de fichiers mise en place depuis des décennies. FTP échange les données via deux canaux séparés : le canal de commande (qui authentifie l'utilisateur) et le canal de données (qui transfère les fichiers).

Aucun des deux canaux FTP n'est crypté, l'accès FTP nécessite un nom d'utilisateur et un mot de passe.

SCP (Secure Copy Protocol) est un ancien protocole réseau qui prend en charge les transferts de fichiers entre plusieurs hôtes sur un réseau. Assez proche de FTP, SCP prend cependant en charge des fonctions de cryptage et d'authentification.