Solo Q

JOB 1

- Afficher le manuel de la commande ls
  `ls -h`

- Afficher les fichiers cachés du home de votre utilisateur
  `ls -d .*`

- Afficher les fichiers cachés plus les informations sur les droits sous forme de liste
  `ls -lisa .*`

  - Comment ajouter des options à une commande ?
    On ajoute des options grâce à un ou deux tirets (-)
  - Quelles sont les deux syntaxes principales d'écriture des options pour une commande ?
    Les deux syntaxes principales sont : le tiret simple et le double tirets.

JOB 2

- 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 3

- Installer le paquet “cmatrix”

  Sur debian/ubuntu : `sudo apt install cmatrix`
  Sur archlinux : `sudo pacman -S cmatrix`

- lancer le paquet que vous venez d’installer

  Il suffit d'écrire le nom du paquet en l'occurrence `cmatrix`

- Mettre à jour son gestionnaire de paquets

  ```
  sudo apt-get update
  ```

- Mettre à jour ses différents logiciels

  ```
  sudo apt-get upgrade
  ```

- Télécharger les internets : Google

  ```
  wget
  https://dl.google.com/linux/direct/google-chrome-stable_c
  urrent_amd64.deb
  ```

- Redémarrer votre machine
  pour redémarrer on a le choix entre deux commande :

  ```
  reboot
  shutdown -r now
  ```

  La deuxième étant plus évoluée et dispose de plus d'options.

- éteindre votre machine

```
poweroff
```

JOB 4

- Créer un groupe appelé “Plateformeurs”

```
groupadd Plateformeurs
```

- Créer un utilisateur appelé “User1”

```
useradd user1
```

- Créer un utilisateur appelé “User2”

```
useradd user2
```

- Ajouter “User2” au groupe Plateformeurs

```
gpasswd -a user2 plateformeurs
```

- 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”

```
chown user1 groupes.txt
```

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

```
setfacl -m u:User2r:r droits.txt
```

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

```
chmod o+r groupes.txt
```

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

```
sudo chgrp plateformeurs groupes.txt
```

JOB 5

- 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='apt-get update'
```

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

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

- Ajouter une variable d’environnement qui se nommera “USER” et qui sera égale à votre nom d’utilisateur

```
USER=enzom
```

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

```
gedit .bashrc
exec .bashrc
```

- Afficher les variables d’environnement

```
printenv
```

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

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

JOB 6

Pour accéder au JOB 7 il suffit de faire la commande

```
wget --no-check-certificate 'https://drive.google.com/file/d/1s9ZhRhjo0FXcBNRB5khAGK1jVxkZj6Uk/' tar -xzvf Ghost\ in\ the\ Shell.tar.gz
```

JOB 7 GHOST IN THE SHELL

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

  ```
  touch une_commande.txt ; echo “Je suis votre fichier texte” > une_commande.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 ; wc -l sources.list > nb_lignes.txt
  ```

- Afficher le contenu du fichier source apt et l’enregistrer dans un autre fichier appelé “save_sources”

  ```
  cat /etc/apt/sources.list > save_sources
  ```

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

  ```
  grep -r “alias”
  ```

  La commande complète en entier sera donc :

  ```
  touch une_commande.txt ; echo “Je suis votre fichier texte” > une_commande.txt ;
  ```

```
cd /etc/apt ; wc -l sources.list > nb_lignes.txt ; cat /etc/apt/sources.list > save_sources ; 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 de votre / en enregistrant le résultat dans un fichier "tree.save"

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

- lister les éléments présents dans le dossier courant et utilisé directement le résultat de votre première commande pour compter le nombre d'éléments trouvés

  ```
  ls
  wc tree.save
  ```

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

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

Pour la commande en entier :

```
sudo apt-get install tree ; tree ./ > tree.save & ls ; wc -l tree.save ; apt-get update && apt-get upgrade
```

JOB 8

- Quel est l'intérêt d'utiliser SSH ?

SSH est un environnement crypté c'est-à-dire qu'elle est sécurisée même sur une connexion publique et ouverte.
SSH me permet aussi d'atteindre et de modifier un ordinateur qui ne partage pas la même connexion internet que moi donc un contrôle à distance.

- Est-ce que les clés générées par SSH par défaut sont assez sécurisées ? Justifier votre réponse.

SSH est un système sécurisé qui passe par plusieurs systèmes tel que le "hashing" la "symetric encryption" et la "asymetric encryption".
Néanmoins le mot de passe est unique et ne change pas donc une fuite d'informations peut compromettre la structure.

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

FTP (File Transfer Protocol) : Le protocole de transferts de fichiers FTP, est une méthode de transfert populaire qui existe depuis des décennies. FTP échange des données en utilisant deux canaux distincts : le canal de commande pour authentifier l'utilisateur et le canal de données pour transférer les fichiers. Cependant, ces canaux ne sont pas chiffré donc les données envoyées risquent d'être exploité.

SFTP (Secure File Transfer Protocol) :

SFTP permet d'échanger des données via une connexion SSH qui offre un niveau de protection élevé pour les partages de fichiers entre systèmes, cloud, collaborateurs, etc. Excellente alternative à FTP.
HTTP/HTTPS (Hyper Text Transfer Protocol) : Pierre angulaire du « World Wide Web », HTTP (Hyper Text Transfer Protocol) est le pilier de la communication des données. Il définit

le format des messages par lesquels les navigateurs et les serveurs web communiquent et détermine comment un navigateur doit répondre à une requête.
HTTP utilise TCP (Transmission Control Protocol) comme protocole secondaire, qui est aussi un protocole apatride. Cela signifie que chaque commande est exécutée indépendamment et qu'aucune information de session n'est conservée par le destinataire.
HTTPS (Hyper Text Transfer Protocol Secure) est la version sécurisée de HTTP où les communications sont chiffrées par TLS ou SSL.

AS2,AS3,AS4 (Applicability Statement) :
AS2, AS3 et AS4 sont tous des protocoles utilisés pour envoyer et sécuriser les transferts de fichiers sensibles.