

Recap Linux

Connexion à une machine à distance

```
ssh <username>@<Host> -p <Port>
```

`-i <cle_privee>` : pour se connecter via une clé privée.

Lister les fichiers d'un répertoire

```
ls
```

`-a` : pour afficher tous les fichiers même les fichiers cachés

`-l` : pour afficher les droits (permissions) et les propriétaires des fichiers

Lire le contenu d'un fichier

```
cat <fichier>
```

Ou

```
head <fichier>
```

Rechercher dans un fichier

```
grep <mot_à_chercher> <fichier>
```

Rerchercher des fichiers

```
find <chemin> <OPTIONS>
```

Chemin :

Limiter la recherche à un répertoire spécifique

Voyons d'abord comment limiter la recherche à un répertoire spécifique. Pour **rechercher dans le répertoire courant**, on utilise le point « . » comme chemin d'accès au répertoire :

```
find . <option>
```

Pour **rechercher dans son répertoire personnel**, on utilise le tilde « ~ » comme chemin d'accès au répertoire :

```
find ~ <option>
```

Vous pouvez également rechercher l'ensemble du système à l'aide de find sous Linux. Cependant, en raison du grand nombre de fichiers et éventuellement de répertoires, cela peut prendre beaucoup de temps. Pour **rechercher dans tout le système**, on utilise la barre oblique « / » comme chemin d'accès au répertoire :

```
find / <option>
```

OPTIONS :

- user : pour spécifier l'utilisateur propriétaire du fichier
- group : pour spécifier le groupe propriétaire du fichier
- type f : pour indiquer qu'il s'agit d'un fichier

Pour indiquer le type du fichier

```
file <fichier>
```

Pour afficher une chaîne de caractères

```
echo "chaîne_de_caractères"
```

Pour changer le répertoire

```
cd <Nouveau_Repertoire>
```

Astuces :

- **cd ~** permet d'accéder au répertoire personnel d'un autre utilisateur.
- **cd ..** monte d'un répertoire.
- **cd-** permet de revenir au répertoire précédent.

Pour copier un fichier

```
cp <nom_fichier> <chemin_destination>
```

Pour renommer un fichier

```
mv <nom_ancien> <nouveau_nom>
```

Pour déplacer un fichier

```
mv <nom_fichier> <chemin_destination>
```

Pour supprimer des fichiers dans un répertoire

```
rm <fichier1> <fichier2> <fichier3>
```

Pour créer un répertoire

```
mkdir <nom_du_repertoire>
```

Pour coder/décoder en base 64

```
#Pour coder :  
base64 <fichier_ou_chaine_de_caracteres>  
  
#Pour décoder :  
base64 -d <fichier_ou_chaine_de_caracteres>
```

Pour remplacer des caractères par autres dans un fichier en faisant une translation

```
#Exemple Rot13:  
cat <fichier> | tr 'a-zA-Z' 'n-zA-M]'
```

Pour extraire les chaînes de caractères lisibles à partir d'un fichier

```
strings <fichier>
```

Pour convertir un fichier binaire en un format hexadécimal ou inversement

```
#Pour convertir un fichier binaire en un format hexadécimal  
xxd <fichier>
```

```
# Pour convertir un fichier hexadecimale en un format binaire  
xxd -r <fichier>
```

Pour trier les lignes d'un fichier texte dans un ordre spécifié

```
sort <options> <fichier>
```

Exemples d'options :

- `-r` : pour trier les lignes en ordre inverse.
- `-n` : pour trier les lignes numériquement plutôt qu'alphanumériquement.
- `-k` : pour trier en fonction d'une clé spécifiée. Par exemple, `-k2` trie en fonction de la deuxième colonne.

Pour supprimer les lignes en double ou consécutives dans un fichier texte

```
uniq <options> <fichier>
```

Exemple d'options :

- `-d` : pour afficher uniquement les lignes en double.
- `-c` : pour afficher le nombre d'occurrences de chaque ligne.
- `-u` : pour afficher uniquement les lignes uniques (c'est-à-dire les lignes qui n'apparaissent qu'une seule fois).

Pour comparer deux contenus d'un fichier ligne par ligne

```
diff <fichier1> <fichier2>
```

Pour la compression et la décompression de fichiers

```
# Pour compresser  
gzip <nom_fichier>  
  
# Pour décompresser  
gzip -d <nom_fichier>.gz
```

```
# Pour compresser
bzip2 <nom_fichier>

# Pour décompresser
bzip2 -d <nom_fichier>.bz2
```

```
# Pour décompresser
tar -xvf <nom_fichier>.tar
```

Commandes Réseau

Telnet

Telnet est un protocole de communication réseau qui permet d'établir des connexions distantes avec un serveur distant.

```
telnet <adresse_ip> <port>
```

Netcat

Netcat est un utilitaire réseau polyvalent qui permet d'établir des **connexions TCP/UDP**, d'**écouter des ports**, de **transférer des données**, etc.

```
nc <adresse_ip> <port>
```

OpenSSL et son outil s_client

OpenSSL est une **bibliothèque** qui prend en charge différents protocoles de sécurité, tels que SSL/TLS, et fournit des outils pour effectuer des opérations de cryptographie, générer des clés, des certificats, etc.

s_client est un **outil inclus** dans le paquet OpenSSL qui permet d'établir une **connexion à un serveur distant** en utilisant le protocole **SSL/TLS**.

```
openssl s_client -connect <adresse>:<port>
```

nmap

Nmap (Network Mapper) est un outil open source utilisé pour l'exploration et la sécurisation des réseaux. Il permet d'**analyser les hôtes** et les services réseau, de découvrir les ports ouverts, d'identifier les systèmes d'exploitation, et bien plus encore.

```
nmap <options> <adresse_ip_de_la_cible>
```

Parmi les options :

- `-p` : Spécifie les ports à scanner. Par exemple, `-p 80,443` scanne les ports 80 et 443.
- `-p-` : Scan de tous les ports sur une machine.
- `-p <plage_de_port>` : Scan d'une plage de ports spécifique