TP: Utilisation avancée des commandes Linux pour un ingénieur en cybersécurité

Objectif

Ce TP vise à familiariser un ingénieur en cybersécurité avec les commandes Linux `ls`, `cd`, `mkdir`, `rm`, `cp`, `mv`, et `touch`. Vous apprendrez à naviguer dans le système de fichiers, manipuler les fichiers et les répertoires, et gérer les permissions et les attributs des fichiers de manière sécurisée.

Scénario

Vous êtes un ingénieur en cybersécurité chargé de sécuriser un serveur Linux. Vous devrez organiser des fichiers, configurer des permissions, et gérer les fichiers de log.

Prérequis

- Accès à un terminal Linux
- Compte utilisateur avec des permissions sudo

Partie 1 : Navigation et Inspection

1. **Lister les fichiers et répertoires**
   - Listez tous les fichiers et répertoires dans le répertoire `/var/log`.

     ```
     ls /var/log
     ```

   - Listez les fichiers avec des détails (permissions, propriétaire, taille, date de modification).

     ```
     ls -l /var/log
     ```

   - Affichez les fichiers cachés dans le répertoire `/etc`.

     ```
     ls -a /etc
     ```

   - Listez les fichiers dans `/home` en format lisible par l'humain.

     ```
     ls -lh /home
     ```

2. **Changer de répertoire**
   - Changez de répertoire pour aller dans `/var/log`.

```
cd /var/log
```

- Retournez dans votre répertoire personnel.

```
cd ~
```

- Allez dans le répertoire parent de votre répertoire actuel.

```
cd ..
```

- Retournez dans le répertoire précédent.

```
cd -
```

Partie 2 : Création et Gestion de Répertoires

1. **Créer des répertoires**

   - Créez un répertoire `cybersec` dans votre répertoire personnel.

   ```
   mkdir ~/cybersec
   ```

   - Créez plusieurs répertoires en une seule commande : `logs`, `reports`, et `scripts` à l'intérieur de `cybersec`.

   ```
   mkdir ~/cybersec/logs ~/cybersec/reports ~/cybersec/scripts
   ```

   - Créez une structure de répertoires imbriqués `2024/january/week1` dans `reports`.

   ```
   mkdir -p ~/cybersec/reports/2024/january/week1
   ```

Partie 3 : Création et Gestion de Fichiers

1. **Créer des fichiers**

- Créez un fichier vide `readme.txt` dans `cybersec`.

```
touch ~/cybersec/readme.txt
```

- Créez plusieurs fichiers vides `log1.txt`, `log2.txt`, et `log3.txt` dans `logs`.

```

```

touch ~/cybersec/logs/log1.txt ~/cybersec/logs/log2.txt ~/cybersec/logs/log3.txt

```
ou

 ```sh
mkdir -p ~/cybersec/logs
for i in {1..3}; do touch ~/cybersec/logs/log$i.txt; done
```

- Créez un fichier avec une date spécifique.

```
touch -t 202406290830 ~/cybersec/logs/log1.txt
```

Partie 4 : Manipulation de Fichiers et Répertoires

1. **Copier des fichiers**
   - Copiez `readme.txt` dans le répertoire `scripts`.

```
cp ~/cybersec/readme.txt ~/cybersec/scripts/
```

   - Copiez tous les fichiers `.txt` de `logs` vers `reports/2024/january/week1`.

```
cp ~/cybersec/logs/*.txt
~/cybersec/reports/2024/january/week1/
```

2. **Déplacer et renommer des fichiers**
   - Déplacez `log1.txt` de `logs` vers `scripts` et renommez-le en `script_log1.txt`.

```

```
```

```
mv ~/cybersec/logs/log1.txt ~/cybersec/scripts/script_log1.txt
```

- Renommez `readme.txt` en `README.md`.

```
mv ~/cybersec/readme.txt ~/cybersec/README.md
```

Partie 5 : Suppression de Fichiers et Répertoires

1. **Supprimer des fichiers et répertoires**
   - Supprimez le fichier `log2.txt` dans `logs`.

```
rm ~/cybersec/logs/log2.txt
```

   - Supprimez le répertoire `week1` et tout son contenu.

```
rm -rf ~/cybersec/reports/2024/january/week1
```

   - Supprimez tous les fichiers `.txt` dans `logs`.

```
rm ~/cybersec/logs/*.txt
```

Partie 6 : Permissions et Propriétés des Fichiers

1. **Changer les permissions des fichiers**
   - Rendre `README.md` exécutable par le propriétaire uniquement.

```
chmod 700 ~/cybersec/README.md
```

   - Donner des permissions de lecture et d'exécution au groupe et aux autres pour tous les fichiers dans `scripts`.

```
chmod -R 755 ~/cybersec/scripts
```

2. **Changer le propriétaire et le groupe**

- Changez le propriétaire de `README.md` à `root` et le groupe à `adm`.

```
sudo chown root:adm ~/cybersec/README.md
```

Partie 7 : Sécurité Avancée

1. **Recherche de fichiers spécifiques**
   - Trouvez tous les fichiers de plus de 10 Mo dans `/var/log`.

```
find /var/log -type f -size +10M
```

2. **Monitoring des logs**
   - Surveillez les changements en temps réel dans le fichier `syslog`.

```
tail -f /var/log/syslog
```

3. **Audit de sécurité**
   - Créez un fichier d'audit contenant les permissions des fichiers dans `/etc`.

```
ls -l /etc > ~/cybersec/audit_$(date +%Y-%m-%d).txt
```

Partie 8 : Nettoyage

1. **Nettoyage des fichiers et répertoires créés**
   - Supprimez tous les répertoires et fichiers créés pendant ce TP.

```
rm -rf ~/cybersec
```