TP : Utilisation avancée de `find`, `grep`, `less`, `tail`, `cat` et `more` pour un ingénieur en cybersécurité

Partie 1 : Recherche de Fichiers avec `find`

1. Rechercher tous les fichiers `.log` dans le répertoire `/var/log` :

```
find /var/log -type f -name "*.log"
```

2. Rechercher tous les fichiers modifiés dans les 7 derniers jours dans `/etc` :

```
find /etc -type f -mtime -7
```

3. Rechercher tous les fichiers de plus de 10 Mo dans `/var/log` :

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

4. Rechercher tous les fichiers appartenant à l'utilisateur `root` dans `/var/log` :

```
find /var/log -type f -user root
```

Partie 2 : Recherche de Contenu dans les Fichiers avec `grep`

1. Rechercher le mot "error" dans tous les fichiers `.log` dans `/var/log` :

```
grep -r "error" /var/log/*.log
```

2. Rechercher le mot "failed" dans les fichiers de configuration dans `/etc` et afficher les numéros de ligne :

```
grep -rn "failed" /etc
```

3. Rechercher les adresses IP dans un fichier log spécifique :

```
grep -oE '\b([0-9]{1,3}\.){3}[0-9]{1,3}\b' /var/log/syslog
```

Partie 3 : Visualisation avec `less` et `more`

1. Afficher le contenu de `/var/log/syslog` avec `less` :

```
less /var/log/syslog
```

- Utilisez `/error` pour rechercher "error"
- Appuyez sur `q` pour quitter

2. Afficher le contenu de `/etc/passwd` avec `more` :

```
more /etc/passwd
```

- Utilisez `Espace` pour avancer d'une page
- Appuyez sur `q` pour quitter

Partie 4 : Surveillance de Fichiers avec `tail`

1. Afficher les 20 dernières lignes de `/var/log/syslog` :

```
tail -n 20 /var/log/syslog
```

2. Suivre les nouvelles lignes ajoutées à `/var/log/syslog` en temps réel :

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

3. Suivre les nouvelles lignes ajoutées à plusieurs fichiers log en temps réel :

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

Partie 5 : Affichage et Manipulation avec `cat`

1. Afficher le contenu de `/etc/hosts` :

```
cat /etc/hosts
```

2. Afficher le contenu de plusieurs fichiers de configuration :

```
cat /etc/hosts /etc/resolv.conf
```

3. Combiner plusieurs fichiers de log en un seul fichier :

```
cat /var/log/syslog /var/log/auth.log > /tmp/combined_logs.log
```

4. Afficher les numéros de ligne dans un fichier de configuration :

```
cat -n /etc/hosts
```

Partie 6 : Combinatoires Avancées

1. Rechercher les fichiers `.log` modifiés dans les 7 derniers jours et contenant "error" :

```
find /var/log -type f -name "*.log" -mtime -7 -exec grep -H "error" {}
\;
```

2. Suivre les erreurs en temps réel dans les logs du système et les afficher avec `less` :

```
tail -f /var/log/syslog | grep --line-buffered "error" | less
```

3. Rechercher les fichiers `.conf` dans `/etc` et les visualiser un par un avec `more` :

```
find /etc -type f -name "*.conf" -exec more {} \;
```