

## TP - Maîtrise du CMD Windows : Administration système et réseau

### Objectifs pédagogiques

- Maîtriser les commandes essentielles de l'invite de commandes Windows
- Comprendre la gestion des fichiers, processus et réseaux
- Développer des compétences en troubleshooting système

### Exercice 1 : Prise en main de l'environnement CMD

---

#### 1.1 Lancement et configuration

- Ouvrez CMD en tant qu'administrateur :
  - Win + X → Invite de commandes (admin) **OU**
  - Win + R → cmd → Ctrl + Shift + Entrée

#### Tâches :

1. Vérifiez votre dossier courant avec **echo %CD%**
2. Affichez la version de Windows avec ver
3. Capture d'écran montrant ces informations

#### 1.2 Personnalisation de l'environnement

- Tapez **color 0A**
- Tapez **prompt \$T [\$P]\$G**
- Tapez **title Session\_Admin\_CMD**

#### Questions :

- Que fait la commande color ?
- Comment le prompt a-t-il changé ?
- À quoi sert la commande title ?

### Exercice 2 : Exploration avancée du système de fichiers

---

#### 2.1 Navigation et arborescence

#### Tâches :

1. Créez la structure suivante :

```
TP_CMD
├── Documents/
│   ├── Textes/
│   ├── Images/
│   ├── Archives/
│   └── Temp/
```

#### 2.2 Attributs de fichiers avancés

```
echo CONTENU_SECRET > Documents\fichier_cache.txt
dir
attrib +H Documents\fichier_cache.txt
dir Documents
```

## ***dir Documents /A***

### **Questions :**

- Que signifient les attributs +H ?
- Comment afficher les fichiers cachés avec dir ?

## **Exercice 3 : Gestion des processus et services**

---

### **3.1 Analyse des processus système**

***tasklist /FO TABLE /V***

#### **Tâches :**

1. Lancez le Bloc-notes et Paint
2. Identifiez leurs PID avec :

***tasklist | findstr "notepad mspaint"***

### **3.2 Gestion fine des processus**

***:: Tuer un processus par PID***

***taskkill /PID [PID\_NUMBER] /F***

***:: Tuer par nom d'image***

***taskkill /IM notepad.exe /T***

#### **Questions :**

- Quelle est la différence entre /F et /T ?
- Pourquoi faut-il être prudent avec taskkill ?

## **Exercice 4 : Diagnostic réseau avancé**

---

### **4.1 Analyse complète de la configuration**

***ipconfig /all***

***ou***

***netsh interface ip show config***

#### **Questions :**

- Quelle est votre adresse MAC ?
- Le DHCP est-il activé ?
- C'est quoi un DHCP ?
- Quel serveur DNS utilisez-vous ?

### **4.2 Tests de connectivité**

***ping 8.8.8.8 -n 4***

***ping google.com***

***tracert google.com***

***pathping google.com***

#### **Tâches :**

1. Explique le résultat du premier ping

- Réponse de 8.8.8.8 : octets=32 temps=12 ms TTL=115
2. Comparez les résultats de tracert et pathping
  3. Testez la résolution DNS avec nslookup google.com

#### 4.3 Statistiques réseau

***netstat -ano***

***netstat -an | find ":80"***

***netstat -e 5***

**Questions :**

- Que montre netstat -ano ?
- Comment identifier les connexions établies sur le port 80 ?

### Exercice 5 : Scripting basique et automatisation

---

#### 5.1 Création d'un script de sauvegarde

Créez un fichier sauvegarde.bat :

***@echo off***

***echo === SAUVEGARDE DOSSIERS IMPORTANTS ===***

***set BACKUP\_DIR=%USERPROFILE%\Backup\_%DATE%***

***mkdir "%BACKUP\_DIR%"***

***xcopy "%USERPROFILE%\Documents\\*.txt" "%BACKUP\_DIR%\Textes\" /S /I /Y***

***xcopy "%USERPROFILE%\Desktop\\*.pdf" "%BACKUP\_DIR%\PDF\" /S /I /Y***

***echo Sauvegarde terminee: %BACKUP\_DIR%***

***dir "%BACKUP\_DIR%" /S***

***pause***

1. Que fait la commande @echo off et pourquoi est-elle utile ici ?
2. Que fait la commande set BACKUP\_DIR=%USERPROFILE%\Backup\_%DATE% ?
  - Que contient la variable %USERPROFILE% ?
  - Que contient la variable %BACKUP\_DIR% après son exécution ?
3. Que fait mkdir "%BACKUP\_DIR%" ?
  - Que se passerait si le dossier existait déjà ?
4. Que fait xcopy "%USERPROFILE%\Documents\\*.txt" "%BACKUP\_DIR%\Textes\" /S /I /Y ?
  - Que signifient les options /S /I /Y ?
5. Pourquoi crée-t-on deux dossiers différents (Textes et PDF) ?
6. Que fait la commande dir "%BACKUP\_DIR%" /S ?

7. Quel est le rôle de pause ? Que se passerait si on le supprimait ?

### Améliorations

1. Comment pourriez-vous **sauvegarder d'autres types de fichiers** (images, vidéos) ?
2. Comment rendre le script **plus robuste** si un fichier est en cours d'utilisation ou s'il y a un problème de droits ?
3. Comment automatiser ce script pour qu'il **s'exécute tous les jours** sans intervention manuelle ?

## 5.2 Surveillance système

Créez monitor.bat :

```
@echo off
:loop
cls
echo === MONITORING SYSTEME ===
echo Date: %DATE% - Heure: %TIME%
echo.
echo === PROCESSUS ===
tasklist /FO TABLE | findstr /I "chrome firefox"
echo.
echo === CONNEXIONS RESEAU ===
netstat -an | find ":80"
timeout /t 10 /nobreak
goto loop
```

1. Que fait la commande @echo off ? Pourquoi est-elle utile dans ce script ?
2. Quelle est la fonction de l'étiquette :loop et du goto loop ?
3. Que se passe-t-il quand on exécute cls ? Pourquoi est-ce important dans ce script ?
4. Que vont afficher %DATE% et %TIME% ? Que se passerait si on supprimait cette ligne ?
5. À quoi sert tasklist /FO TABLE | findstr /I "chrome firefox" ?
  - Que se passerait si on remplaçait "chrome firefox" par "notepad" ?
6. Que fait la commande netstat -an | find ":80" ? Que signifie le :80 ?
7. Quel est le rôle de timeout /t 10 /nobreak ? Que se passerait si on mettait /t 0 ?
8. Pourquoi le script utilise-t-il une boucle infinie ? Quels sont les avantages et inconvénients d'un tel fonctionnement ?

### Améliorations

1. Comment pourriez-vous modifier le script pour surveiller **plusieurs ports réseau** en même temps, par exemple 80 et 443 ?

2. Comment pourriez-vous faire en sorte que le script **enregistre l'historique** des processus et connexions dans un fichier texte pour consultation ultérieure ?
3. Comment pourriez-vous modifier le script pour qu'il **s'arrête automatiquement** après un certain nombre de cycles ou après un certain temps ?
4. Que pourriez-vous faire pour rendre l'affichage **plus lisible ou esthétique**, par exemple avec des couleurs différentes pour les sections ?