

# METGY LEO SIO1

## Commandes CMD Essentielles du Support Informatique

Ce TD a pour but de familiariser les étudiants avec les commandes essentielles de l'invite de commandes Windows (CMD) utilisées quotidiennement en support informatique : diagnostic système, dépannage réseau, gestion des utilisateurs, réparation et gestion de session.

Chaque section présente des commandes clés suivies d'exercices d'application.

### 1. Information et Diagnostic du Système

---

Ces commandes permettent de collecter des informations sur la configuration matérielle, logicielle et l'état général du poste.

Commande	Fonction
<b>SYSTEMINFO</b>	Affiche des informations détaillées sur l'OS, les mises à jour et la configuration matérielle.
<b>HOSTNAME</b>	Affiche le nom du poste local.
<b>TASKLIST</b>	Liste l'ensemble des processus en cours d'exécution.

Testez les commandes suivantes

### 2. Dépannage Réseau

---

Commandes recourues pour analyser la connectivité et les flux réseau.

Commande	Fonction
<b>PING</b>	Teste la connectivité réseau vers une machine.
<b>TRACERT</b>	Montre les routeurs traversés jusqu'à une destination.
<b>IPCONFIG /ALL</b>	Affiche la configuration réseau complète (DNS, IP, MAC...).
<b>NETSTAT - ANO</b>	Affiche les connexions actives, les ports d'écoute et les PIDs associés.
<b>ARP -A</b>	Affiche le cache ARP (association IP ↔ MAC).

Testez les commandes suivantes

### 3. Gestion des Utilisateurs et de la Sécurité

---

Commandes utilisées pour l'administration locale des comptes.

Commande	Fonction
<b>NET USER</b>	Affiche les utilisateurs locaux ou permet d'en ajouter/supprimer.

<b>NET LOCALGROUP ADMINISTRATORS</b>	Ajoute un utilisateur au groupe Administrateurs.
<b>WHOAMI</b>	Affiche l'utilisateur actuellement connecté ainsi que son domaine.

Testez les commandes suivantes

#### 4. Réparation Système et Gestion des Processus

Commandes destinées à vérifier l'intégrité du système ou à gérer des processus problématiques.

Commande	Fonction
<b>CHKDSK /F</b>	Analyse et répare les erreurs sur un disque.
<b>SFC /SCANNOW</b>	Vérifie et répare les fichiers système corrompus.
<b>TASKKILL /PID</b>	Termine un processus en fonction de son identifiant (PID).
<b>TREE</b>	Affiche la structure des répertoires en arborescence.

Testez les commandes suivantes

# Exercices

## 1. Diagnostic et Information

---

### Situation :

Un professeur signale que son ordinateur est « extrêmement lent » et démarre anormalement. Avant d'envisager un remplacement ou une opération lourde, vous souhaitez vérifier **les processus en cours**, afin d'identifier une éventuelle surcharge CPU ou un programme bloqué.

### Question :

Quelle commande utilisez-vous pour **répertorier l'ensemble des processus actuellement actifs** sur le poste afin d'effectuer un premier diagnostic ?

C'est la commande **tasklist** qui permet d'afficher la liste des processus actifs.

```
C:\Users\etudinfo>tasklist

Nom de l'image          PID Nom de la sessio Numéro de s Utilisation
=====
System Idle Process      0 Services              0           8 Ko
System                   4 Services              0        6 588 Ko
Secure System           56 Services              0       37 932 Ko
Registry                116 Services              0       48 948 Ko
smss.exe                 420 Services              0        1 208 Ko
csrss.exe                 604 Services              0        5 996 Ko
wininit.exe              688 Services              0        7 156 Ko
services.exe             784 Services              0       14 368 Ko
lsass.exe                 848 Services              0       3 804 Ko
```

## 2. Dépannage Réseau & Authentification

---

### Situation :

Un utilisateur n'arrive plus à accéder à son dossier personnel sur le serveur et pense « ne pas être reconnu par le domaine ».

Avant de vérifier côté Active Directory, vous devez d'abord confirmer **le compte réellement utilisé** par la session, ainsi que le domaine auquel il appartient.

### Question :

Quelle commande permet d'afficher **l'utilisateur connecté** ainsi que **le domaine de connexion** ?

C'est la commande **whoami** qui permet d'afficher l'utilisateur connecté et le domaine de connexion.

```
C:\Users\etudinfo>whoami
pcr2\etudinfo
```

## 3. Analyse Réseau et Sécurité

---

### Situation :

Vous suspectez qu'un programme inconnu utilise un **port réseau critique** sur un

poste d'un utilisateur.

Pour identifier précisément ce processus, vous devez examiner les **connexions actives**, les **ports ouverts**, et les **PIDs associés** afin de déterminer quel logiciel occupe ce port.

### Question :

Quelle commande permet d'obtenir, en une seule fois, la **liste des connexions actives**, les **ports d'écoute**, et les **processus correspondants** ?

C'est la commande **netstat -ano** qui permet d'obtenir en une seule fois la liste des connexions actives, les ports d'écoute et les processus correspondants.

```
C:\Users\etudinfo>netstat -ano
Connexions actives

Proto  Adresse locale      Adresse distante    État                PID
TCP    0.0.0.0:135          0.0.0.0:0           LISTENING           916
TCP    0.0.0.0:445          0.0.0.0:0           LISTENING            4
TCP    0.0.0.0:902          0.0.0.0:0           LISTENING          4384
TCP    0.0.0.0:912          0.0.0.0:0           LISTENING          4384
TCP    0.0.0.0:5040         0.0.0.0:0           LISTENING          7304
TCP    0.0.0.0:5357         0.0.0.0:0           LISTENING            4
```

## 4. Administration des Comptes Utilisateurs

---

### Situation :

Un ancien employé du lycée ou de l'entreprise quitte définitivement l'établissement. Conformément aux procédures internes, son compte local doit être **supprimé** des postes Windows concernés.

### Question :

Quelle commande supprime le compte local nommé **ancienemploye** ?

C'est la commande **net user ancienemploye /delete** qui permet de supprimer le compte local ancienemploye.

## 5. Identification du Poste dans un Parc Informatique

---

### Situation :

Tu dois inventorier rapidement les postes d'une salle informatique pour préparer une mise à jour Windows.

Avant de lancer le script automatisé, tu dois relever **le nom de la machine** afin de t'assurer que tu opères sur le bon poste.

### Question :

Quelle commande permet d'afficher le nom du poste sur lequel vous êtes connecté ?

C'est la commande **hostname** qui permet d'afficher le nom du poste.

```
C:\Users\etudinfo>hostname
PCR2
```

## 6. Vérification Complète de la Configuration Réseau

---

### Situation :

Un élève n'arrive plus à imprimer depuis son poste. Tu suspectes une mauvaise configuration réseau (DNS ou passerelle).

Pour confirmer tes soupçons, tu dois examiner **l'intégralité** de la configuration réseau du PC.

### Question :

Quelle commande permet d'afficher l'ensemble des paramètres réseau (adresse IP, DNS, passerelle, MAC, etc.) ?

C'est la commande **ipconfig /all** qui permet d'afficher l'ensemble des paramètres réseau.

```
C:\Users\etudinfo>ipconfig /all

Configuration IP de Windows

    Nom de l'hôte . . . . . : PCR2
    Suffixe DNS principal . . . . . :
    Type de noeud . . . . . : Hybride
    Routage IP activé . . . . . : Non
    Proxy WINS activé . . . . . : Non
    Liste de recherche du suffixe DNS.: sio.edu

Carte Ethernet Eth 1 - Realtek :

    Suffixe DNS propre à la connexion. . . : sio.edu
    Description. . . . . : Realtek PCIe GbE Family Controller
    Adresse physique . . . . . : 18-60-24-F4-CF-5C
    DHCP activé. . . . . : Oui
    Configuration automatique activée. . . : Oui
    Adresse IPv6 de liaison locale. . . . : fe80::dc7:4b5e:77de:d412%4(préfééré)
    Adresse IPv4. . . . . : 192.168.28.52(préfééré)
    Masque de sous-réseau. . . . . : 255.255.255.0
    Bail obtenu. . . . . : lundi 8 décembre 2025 12:07:13
    Bail expirant. . . . . : lundi 8 décembre 2025 18:05:28
    Passerelle par défaut. . . . . : 192.168.28.253
    Serveur DHCP . . . . . : 192.168.28.253
```

## 7. Analyse du Chemin Réseau vers un Serveur

---

### Situation :

Le serveur pédagogique srv-pedago semble répondre très lentement à certains utilisateurs.

Tu dois déterminer si un routeur intermédiaire provoque une latence anormale.

### Question :

Quelle commande affiche **toutes les étapes** (sauts) traversées par les paquets pour atteindre une machine distante ?

C'est la commande **tracert + nom de domaine** → exemple : **tracert google.com** qui affiche toutes les étapes traversées par les paquets pour atteindre une machine distante.

```

C:\Users\etudinfo>tracert google.com

Détermination de l'itinéraire vers google.com [142.250.179.110]
avec un maximum de 30 sauts :

  1      1 ms    <1 ms    <1 ms    192.168.28.253
  2      1 ms     1 ms     1 ms     10.96.9.245
  3     29 ms    15 ms    12 ms    172.18.128.93
  4     10 ms    10 ms    10 ms    10.251.0.2
  5     11 ms    11 ms    11 ms    routeur-upjv.ac-amiens.fr [195.221.156.15]
  6     13 ms    13 ms    12 ms    194.167.1.141
  7     13 ms    14 ms    13 ms    vl221-be2-ren-nr-compiegne-rtr-091.noc.renater.fr [193.51.181.190]
  8     24 ms    15 ms    16 ms    xe-0-0-8-ren-nr-paris2-rtr-131.noc.renater.fr [193.51.177.206]
  9     18 ms    16 ms    16 ms    192.178.70.144
 10     14 ms    15 ms    15 ms    72.14.233.195
 11     19 ms    17 ms    23 ms    142.251.49.135
 12     17 ms    17 ms    19 ms    par21s20-in-f14.1e100.net [142.250.179.110]

Itinéraire déterminé.

```

## 8. Vérification de l'intégrité du système

---

### Situation :

Une machine présente des erreurs étranges et certains services refusent de démarrer. Tu suspectes un fichier système corrompu.

### Question :

Quelle commande analyse l'intégrité des fichiers système et tente de les réparer automatiquement ?

C'est la commande **sfc /scannow** qui permet d'analyser l'intégrité des fichiers système et tente de les réparer automatiquement.

## 9. Détection d'erreurs sur un disque

---

### Situation :

Un professeur se plaint d'erreurs répétées lors de l'enregistrement de documents. Avant de remplacer le disque, tu veux réaliser une **analyse et réparation automatique** du volume.

### Question :

Quelle commande permet d'analyser le disque C: et de réparer les erreurs détectées ?

C'est la commande **chkdsk C : /f** qui permet d'analyser le disque C : et de réparer les erreurs détectées.

## Script 1 : Audit rapide d'un poste utilisateur

---

Réaliser un diagnostic express d'un poste Windows afin d'identifier les principales causes de lenteur ou d'anomalies réseau.

Aucune interaction utilisateur (script autonome).

Le script doit afficher

- Affichage de l'utilisateur connecté.
- Liste des processus lourds.
- Liste des partages réseau montés.
- Connexions réseau établies (pour suspicion malware).

```
@echo off
echo =====
echo Utilisateur connecte:
whoami
echo =====
echo Liste des processus lourds (top 5):
tasklist | findstr /i "0" | findstr /i "1" | findstr /i "2" | findstr /i "3" | findstr /i "4" | findstr /i "5" | findstr /i "6" | findstr /i "7" | findstr /i "8" | findstr /i "9"
echo =====
echo Partages reseau montes:
net use
echo =====
echo Connexions reseau etablies:
netstat -an | findstr "ESTABLISHED"
echo =====
echo Fin du diagnostic.
pause
```

## Script 2 : Onboarding utilisateur

---

Automatiser la création d'un nouvel utilisateur local et la configuration initiale de son environnement réseau.

Déploiement de nouveaux employés ou stagiaires dans une PME ou un établissement scolaire nécessitant un onboarding rapide.

Le script saisie les données suivantes :

- Nom du nouvel utilisateur.
- Mot de passe temporaire.

Le script doit effectuer :

- La création du compte.
- L'Ajout à un groupe spécifique.
- Le montage automatique du lecteur réseau personnel.

```
@echo off
echo =====
echo ONBOARDING UTILISATEUR
echo =====
set /p USERNAME="Nom utilisateur: "
set /p PASSWORD="Mot de passe: "
echo.
echo Creation du compte...
net user %USERNAME% %PASSWORD% /add
echo.
echo Ajout au groupe Utilisateurs...
net localgroup Utilisateurs %USERNAME% /add
echo
echo Montage lecteur reseau Z:...
net use Z: \\serveur\partage\%USERNAME% /persistent:yes
echo.
echo Onboarding termine
pause
```