

# APPROCHE THEORIQUE ET PRATIQUE DE TCP/IP

## Sommaire :

Script automatisé :	2
---------------------	---



.....	3
Exercice 3 : Découverte TCP-IP .....	4
3.2 : Préparation et outils : .....	4
3.3.2 : Récupération des informations en mode commande : .....	4
3.3.3 Accès aux informations en mode graphique .....	7
4 : Utiliser Windows PowerShell : .....	12
4.3 Commandes PowerShell et Invite de commande : .....	12
4.4 : Explorez les applets de commande : .....	13
4.5 : Commande Netstat avec PowerShell : .....	13
4.6 Videz la corbeille avec PowerShell : .....	15
5 : Exercices de calcul de réseaux : .....	19

## Script automatisé :

Pour ce TP, certaines activités ne peuvent pas se faire à domicile en raison des limitations techniques ou des ressources nécessaires. Par conséquent, une partie du travail doit être réalisée en classe pour garantir la continuité et la bonne progression des activités. Afin de faciliter le suivi de cette progression et de ne pas perdre les étapes déjà accomplies, j'ai élaboré un script automatisé.

Ce script a pour but de suivre et d'enregistrer chacune des étapes du TP dans un fichier texte. À chaque nouvelle action ou étape complétée, le script met à jour ce fichier, permettant ainsi de reprendre facilement là où nous nous étions arrêtés, que ce soit en classe ou à domicile. Il permet de :

1. Enregistrer la progression actuelle.
2. Gérer les différentes étapes à effectuer pour le TP.
3. Garantir que toutes les parties du TP soient complétées de manière ordonnée et traçable.

```

1  D:\M Drogue\TP 2\src\python2.pyw - Sublime Text (UNREGISTERED)
2  File Edit Selection Find View Goto Tools Project Preferences Help
3
4  python2.pyw
5
6  1 import tkinter as tk
7   from tkinter import ttk
8  import subprocess
9  import threading
10 import time
11 import os
12
13 # Création de la classe principale de l'application
14 class NetworkInfoApp:
15     def __init__(self, master):
16         self.master = master
17         self.master.title("Collecte des Informations Réseau")
18         self.master.geometry("500x400")
19
20         # Variable pour suivre la progression
21         self.progress = 0
22
23         # Configuration du style de la barre de progression
24         self.style = ttk.Style()
25         self.style.theme_use('clam')
26         self.style.configure("blue.Horizontal.TProgressbar", foreground='blue', background='blue')
27
28         # Création des widgets
29         self.create_widgets()
30
31         # Lancement du thread pour la collecte des informations
32         self.thread = threading.Thread(target=self.collect_info)
33         self.thread.start()
34
35     def create_widgets(self):
36         # Label de titre
37         self.label = tk.Label(self.master, text="Collecte des Informations en cours...", font=("Arial", 14))
38         self.label.pack(pady=10)
39
40         # Barre de progression
41         self.progressbar = ttk.Progressbar(self.master, style="blue.Horizontal.TProgressbar", orient="horizontal", length=400, mode="determinate")
42         self.progressbar.pack(pady=10)
43         self.progressbar["maximum"] = 100
44
45         # Zone de texte pour afficher les logs
46         self.text_area = tk.Text(self.master, height=8, width=60)
47         self.text_area.pack(pady=10)
48         self.text_area.insert(tk.END, "Démarrage de la collecte...\n")
49         self.text_area.config(state=tk.DISABLED)
50
51     def collect_info(self):
52         # Chemin du fichier de sortie
53         output_file = "informations_systeme.txt"
54
55         # Ouvrir le fichier en écriture
56         with open(output_file, "w", encoding="utf-8") as f:
57             # Section 1: Informations IPConfig
58             self.update_status("Collecte des Informations IPConfig...")
59             ipconfig_data = subprocess.run("ipconfig /all").stdout
60             f.write("== Informations IPConfig ==\n")
61             f.write(ipconfig_data + "\n\n")
62             self.increment_progress()
63
64             # Section 2: Variables d'environnement
65             self.update_status("Collecte des variables d'environnement...")
66             set_data = subprocess.run("set").stdout
67             f.write("== Variables d'environnement ==\n")
68             f.write(set_data + "\n\n")
69             self.increment_progress()
70
71             # Section 3: Informations Netstat
72             self.update_status("Collecte des Informations Netstat...")
73             netstat_data = subprocess.run("netstat -ano").stdout
74             f.write("== Informations Netstat ==\n")
75             f.write(netstat_data + "\n\n")
76             self.increment_progress()

```

Le code commence par l'initialisation et la gestion de l'interface utilisateur grâce aux modules `tkinter` et `ttk`. Le constructeur `\_\_init\_\_()` crée la fenêtre principale de l'application, configure la barre de progression et installe les éléments visuels. Il utilise

également un thread pour exécuter la collecte des informations réseau en arrière-plan, assurant ainsi que l'interface utilisateur reste réactive et ne se bloque pas pendant l'exécution des tâches.

Ensuite, la méthode `create_widgets()` s'occupe de la création des composants graphiques, tels que le label de titre, la barre de progression personnalisée à l'aide de `tkk.Progressbar`, et une zone de texte pour afficher les logs. L'utilisation de `tkk.Style()` permet de définir un style visuel pour la barre de progression, offrant une meilleure personnalisation et lisibilité. Ces widgets permettent à l'utilisateur de suivre l'avancement de la collecte des informations en temps réel.

La collecte des informations système et réseau est réalisée par la méthode `collect_info()`, qui exécute des commandes telles que `ipconfig`, `netstat` et `ping` en utilisant le module `subprocess`. Ces commandes sont exécutées dans un thread parallèle grâce à `threading.Thread`, garantissant que l'interface reste fluide pendant la collecte. Chaque étape de collecte est enregistrée dans un fichier texte, et la barre de progression est mise à jour pour refléter l'état actuel de la collecte. Le module `os` est également utilisé pour gérer l'enregistrement des résultats dans le fichier système.

Enfin, la méthode `run_command()` exécute chaque commande système à l'aide de `subprocess.check_output()` pour récupérer et afficher les résultats. Pendant ce temps, la méthode `increment_progress()` met à jour la barre de progression à chaque étape accomplie. Un délai simulé est introduit avec `time.sleep(1)` pour représenter le temps nécessaire à l'exécution de chaque tâche, ce qui renforce l'interactivité et la clarté pour l'utilisateur.

Les modules utilisés (`tkinter`, `ttk`, `subprocess`, `threading`, `time`, et `os`) sont tous essentiels pour garantir une application fonctionnelle et réactive, capable de collecter et d'enregistrer des informations système tout en offrant un retour visuel à l'utilisateur.



## Introduction :

Dans ce TP, nous allons découvrir le protocole TCP/IP en utilisant des commandes comme « ipconfig », « ping » et « netstat ». Nous utiliserons aussi des commandes PowerShell pour gérer les connexions et les processus du système. De plus, nous ferons des calculs de sous-réseaux pour mieux comprendre comment les adresses IP sont organisées. Nous travaillerons à la fois sur un réseau réel, celui du BTS, et sur le simulateur Cisco Packet Tracer pour bien comprendre chaque manipulation.

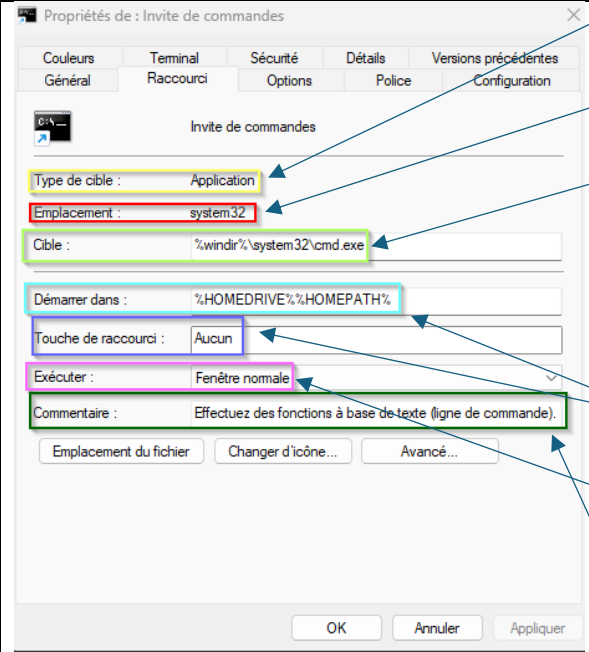
## Exercice 3 : Découverte TCP-IP

### 3.2 : Préparation et outils :

#### 3.3.2 : Récupération des informations en mode commande :

Le chemin d'accès est:

C:\Users\UTI029\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\System Tools



The screenshot shows the 'Properties of Command Prompt' dialog box. The 'Terminal' tab is selected. The 'Inviter de commandes' section contains the following fields:

- Type de cible : Application
- Emplacement : system32
- Cible : %windir%\system32\cmd.exe
- Démarrer dans : %HOMEDRIVE%\%HOMEPATH%
- Touche de raccourci : Aucun
- Exécuter : Fenêtre normale
- Commentaire : Effectuez des fonctions à base de texte (ligne de commande).

Annotations with arrows point from the text on the right to specific fields in the dialog box:

- Il sert à communiquer des informations sur la nature du document. (points to 'Type de cible')
- L'emplacement permet d'indiquer l'endroit où se trouve l'application. (points to 'Emplacement')
- C'est le fichier dans lequel on retrouve l'application (et tous les autres indispensables de Windows). Il est toujours utilisé pour exécuter l'invite de commande. (points to 'Cible')
- Il indique le répertoire de démarrage. (points to 'Démarrer dans')
- Pour voir quelle touche permet d'ouvrir directement l'application. (points to 'Touche de raccourci')
- Choisir la taille de l'application lorsqu'elle est ouverte. (points to 'Exécuter')
- Résumé de ce que fait l'application. (points to 'Commentaire')

## Carte réseau réelle :

```

Carte Ethernet Ethernet :
Suffixe DNS propre à la connexion. . . : sio.local
Adresse IPv6 de liaison locale. . . . : fe80::dd7c:ed8b:e875:d983%14
Adresse IPv4. . . . . : 172.31.1.172
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . : 172.31.1.254

```

- Suffixe Serveur DNS sert à compléter les noms de domaine.
- Adresse MAC (Media Acces Contrôle) est un identifiant unique servant à identifier un appareil sur un réseau local
- Adresse IP qui sert à identifier le poste sur Internet.
- Masque de sous-réseau sert à définir les limites des sous-réseaux.
- Passerelle par défaut sert à communiquer autre part que dans son réseau local.

DNS (Domain Name System) traduit les noms de domaines en adresse IP.

## Différence entre ipconfig et ipconfig /all :

```

Carte Ethernet Ethernet :
Suffixe DNS propre à la connexion. . . : sio.local
Adresse IPv6 de liaison locale. . . . : fe80::dd7c:ed8b:e875:d983%14
Adresse IPv4. . . . . : 172.31.1.172
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . : 172.31.1.254

```

```

Configuration IP de Windows
Nom de l'hôte . . . . . : B181-102
Suffixe DNS principal . . . . . : sio.local
Type de noeud . . . . . : Hybride
Routage IP activé . . . . . : Non
Proxy WINS activé . . . . . : Non
Liste de recherche du suffixe DNS.: sio.local

Carte Ethernet Ethernet :
Suffixe DNS propre à la connexion. . . : sio.local
Description . . . . . : Intel(R) Ethernet Connection (17) I219-LM
Adresse physique . . . . . : E0-73-E7-B2-64-D7
DHCP activé. . . . . : Oui
Configuration automatique activée. . : Oui
Adresse IPv6 de liaison locale. . . . : fe80::dd7c:ed8b:e875:d983%14(préféré)
Adresse IPv4. . . . . : 172.31.1.172(préféré)
Masque de sous-réseau. . . . . : 255.255.255.0
Bail obtenu. . . . . : vendredi 4 octobre 2024 08:07:21
Bail expirant. . . . . : vendredi 4 octobre 2024 08:24:04
Passerelle par défaut. . . . . : 172.31.1.254
Serveur DHCP . . . . . : 172.31.1.6
IDN DHCPv6 . . . . . : 115373031
GUID de client DHCPv6. . . . . : 00-01-00-01-2C-91-20-A6-E0-73-E7-B2-64-D7
Serveurs DNS. . . . . : 172.31.1.4
NetBIOS sur Tcpip. . . . . : Activé

```

Dans les deux images il y a des suffixes DNS propres à la connexion les adresses IPv4 et IPv6, les masques de sous-réseau et la passerelle par défaut. Dans ipconfig /all il y a en plus le suffixe DNS principal et de recherche, le DHCP et DNS et le nom de l'hôte.

DHCP (Dynamic Host Configuration Protocol) permet de donner une adresse IP automatiquement, une passerelle par défaut et les serveurs DNS.

## Informations sur la configuration IP :

```

Configuration IP de Windows
Nom de l'hôte . . . . . : B181-102
Suffixe DNS principal . . . . . : sio.local
Type de noeud . . . . . : Hybride
Routage IP activé . . . . . : Non
Proxy WINS activé . . . . . : Non
Liste de recherche du suffixe DNS.: sio.local

```

- Pour identifier le poste sur un réseau
- Définir ma méthode de résolution de noms de réseau
- Le poste utilise DNS et WINS pour résoudre les noms de domaines
- Le poste ne peut pas servir de routeur
- Le proxy n'aide pas WINS à résoudre les noms NetBIOS
- Compléter les noms de domaine partiels

WINS (Windows Internet Name Service) traduit les noms NetBIOS en adresses IP dans les réseaux, il ressemble au DNS (utilisé pour les noms de domaine internet).

### 3.3.2.1 : Déterminer les paramètres réseau d'un poste :

Nom de poste client (nom NetBIOS)	B181-102
Nom de domaine	sio.local
WINS est-il activé ?	Proxy WINS activé . . . . . : Non
Adresse IP du serveur WINS, si actif	Il n'est pas actif

NetBIOS (Network Basic Input/Output System) est plusieurs interfaces et de services pour que des ordinateurs puissent communiquer sur un réseau local.

### 3.3.2.2 : Vérifier les paramètres TCP/IP :

Comment la station obtient-elle son adresse IPv4 ?	Grâce au DHCP qui en attribue une automatiquement
Adresse IPv4 de la station	172.31.1.172
Masque de sous-réseau	255.255.255.0
Passerelle par défaut	172.31.1.254
DNS est-il activé ?	Oui car les serveurs DNS sont listés
Adresse IP du serveur DNS	172.16.40.1
Durée du bail si DHCP activé	8 jours
Comment la station obtient-elle son adresse IPv6 ?	Grâce à DHCP qui en attribue une automatiquement
Adresse IPv6 de la station	fe80::dd7c:ed8b:e875:d983%14
IAID DHCP v6	115373031
DUID de client DHCP v6	00-01-00-01-2C-91-20-A6-E0-73-E7-B2-64-D7

DHCP (Dynamic Host Configuration Protocol) permet de donner une adresse IP automatiquement, une passerelle par défaut et les serveurs DNS.

### Questions :

-L'adresse IP sert à amener les paquets sur le réseau, sans elle, le poste ne peut pas aller sur internet. De plus, les adresses IP sont reliées à un fournisseur d'accès internet.

-L'adresse MAC est reliée à une interface réseau. L'ordinateur peut en avoir plusieurs donc plusieurs adresses MAC.

L'adresse MAC (Media Access Control) sert à identifier le poste et à communiquer sur un réseau local.

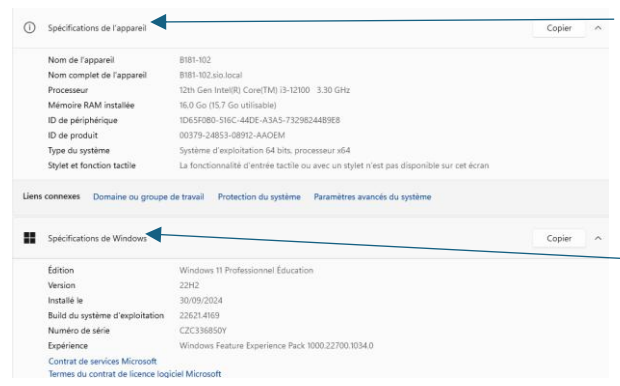
- L'adresse MAC est aussi appelée l'adresse Ethernet (les plus couramment utilisées) ou adresse de couche 2 (là où elles interviennent).

- IAID (Identity Association Identifier) permet d’identifier une adresse IPv6 avec une interface réseau. Et DUID (DHCP Unique Identifier) permet au serveur DHCP de reconnaître un client spécifique.

COMPUTERNAME	B181-102	C’est pour identifier l’appareil sur un réseau
USERDOMAIN	SIO	C’est le nom du domaine dans lequel il se trouve, pour le localiser plus facilement dans les grandes entreprises
USERDNSDOMAIN	SIO.LOCAL	C’est l’adresse du nom de domaine complet
USERNAME	UTI029	Le nom de l’utilisateur
LOGONSERVER	\\AL-DC-02	C’est pour savoir qui à authentifié l’utilisateur

3.3.3 Accès aux informations en mode graphique

3.3.3.1 Informations système

The screenshot shows the 'Specifications of the device' (Spécifications de l'appareil) and 'Specifications of Windows' (Spécifications de Windows) sections. Hardware details include the device name (B181-102), processor (12th Gen Intel(R) Core(TM) i3-12100), RAM (16.0 Go), and system type (64-bit). Windows details include the edition (Windows 11 Professional Education), version (22H2), and installation date (30/09/2024). Blue arrows point from the text on the right to these two sections.

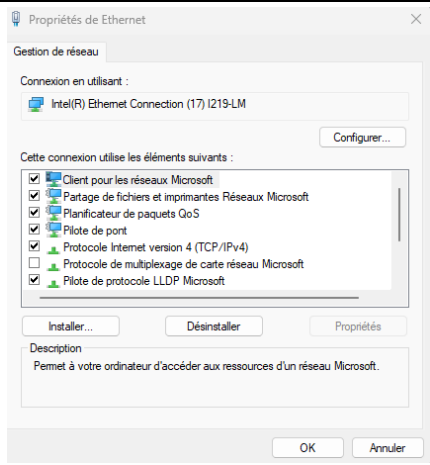
On peut voir les spécifications de l’appareil, son nom, le nom du processeur, la RAM, le système d’exploitation et le processeur.

Et celles de Windows avec son édition, sa version, la date d’installation du système d’exploitation et la build du système d’exploitation.

Mémoire RAM (Random Access Memory) sert de mémoire temporaire le temps que le processeur les traite ou les utilise.

Build est la version exacte du système d’exploitation de l’ordinateur.

3.3.3.2 : Informations réseau

The screenshot shows the 'Ethernet Properties' (Propriétés de Ethernet) window. It lists the network connection as 'Intel(R) Ethernet Connection (17) I219-LM'. Under 'This connection uses the following' (Cette connexion utilise les éléments suivants), several protocols are checked, including 'Client for Microsoft networks' (Client pour les réseaux Microsoft), 'File and printer sharing for Microsoft networks' (Partage de fichiers et imprimantes Réseaux Microsoft), 'QoS Packet Scheduler' (Planificateur de paquets QoS), 'Port driver' (Pilote de port), 'Internet Protocol version 4 (TCP/IPv4)' (Protocole Internet version 4 (TCP/IPv4)), 'Microsoft network card multiplexing protocol' (Protocole de multiplexage de carte réseau Microsoft), and 'Microsoft LLDP protocol driver' (Pilote de protocole LLDP Microsoft). Buttons for 'Install', 'Uninstall', 'Properties', 'OK', and 'Cancel' are visible at the bottom.

On voit la carte réseau utilisée, plusieurs protocoles et les services et composants de la connexion réseau. On a déjà vu les protocoles IPv4 et IPv6 car la fenêtre montre la configuration des protocoles et des services réseaux activés de la connexion Ethernet.



Propriété	Valeur	On voit le modèle de la carte réseau utilisée, l'adresse MAC, le DHCP activé, les informations de l'IPv4 et l'IPv6 et leurs passerelles, le masque de sous-réseau, le bail obtenu et expirant, le DHCP, le DNS, le WINS et le NetBIOS. On a déjà rencontré ces informations dans les paramètres TCP/IP car ça concerne aussi les protocoles IP.
Description	Intel(R) Ethernet Connection (17) I219	
Adresse physique	E0-73-E7-B2-64-D7	
DHCP activé	Oui	
Adresse IPv4	172.31.1.172	
Masque de sous-réseau ...	255.255.255.0	
Bail obtenu	vendredi 11 octobre 2024 08:02:48	
Bail expirant	vendredi 11 octobre 2024 08:52:50	
Passerelle par défaut IPv4	172.31.1.254	
Serveur DHCP IPv4	172.31.1.6	
Serveurs DNS IPv4	172.31.1.4	
	172.31.1.6	
Serveur WINS IPv4		
NetBIOS sur TCP/IP act...	Oui	
Adresse IPv6 locale de li...	fe80::dd7c:ed8b:e875:d983%14	
Passerelle par défaut IPv6		
Serveur DNS IPv6		

### Carte réseau :

Constructeur de la carte réseau	Intel
La carte réseau fonctionne-elle correctement ?	<div>État du périphérique</div> <div>Ce périphérique fonctionne correctement.</div>
Date du pilote	05/05/2024
Indiquez un des fichiers du pilote	<div>Fichiers du pilote :</div> <div>e1d.inf_amd64_dded470da430edc1\e1d.sys</div> <div>e1d.inf_amd64_dded470da430edc1\e1dmsg.dll</div>

### Connexion Ethernet :

sio.local Connecté		^
Paramètres d'authentification		Modifier
Connexion limitée Certaines applications peuvent fonctionner différemment afin de réduire l'utilisation des données lorsque vous êtes connectés à ce réseau.		Désactivé <input type="checkbox"/>
Définir une limite de données permettant de contrôler la consommation des données sur ce réseau		
Attribution d'adresse IP :	Automatique (DHCP)	Modifier
Attribution du serveur DNS :	Automatique (DHCP)	Modifier
Vitesse de connexion (Réception/ Transmission) :	1000/1000 (Mbps)	Copier
Adresse IPv6 locale du lien :	fe80::dd7c:ed8b:e875:d983%14	
Adresse IPv4 :	172.31.1.172	
Serveurs DNS IPv4 :	172.31.1.4 (non chiffré) 172.31.1.6 (non chiffré)	
Suffixe DNS principal :	sio.local	
Fabricant :	Intel	
Description :	Intel(R) Ethernet Connection (17) I219-LM	
Version du pilote :	12.19.2.61	
Adresse physique (MAC) :	E0-73-E7-B2-64-D7	

## Ordinateur :

On voit les détails des informations comme

- La connexion IPv4 et IPv6,
- L'état du média (carte réseau active),
- La durée de la connexion au réseau,
- Sa vitesse à la connexion au réseau
- Les données reçues et
- Les données envoyées

## Tous les contrôleurs de domaine :

Rechercher Utilisateurs, contacts et groupes

Fichier Édition Affichage

Rechercher : Utilisateurs, contacts et groupes Dans : Tout Acti Parcourir...

Utilisateurs, contacts et groupes Avancé

Nom : Description :

Rechercher Arrêter Effacer tout

Résultats de la recherche :

Nom	Type	Description
Bruno DROGUE	Utilisateur	
Samuel GIBERT	Utilisateur	
Interseed	Utilisateur	
vcsa ldap	Utilisateur	Compte dédié pour la synchroni
Admin	Utilisateur	
Administrateur	Utilisateur	Compte d'utilisateur d'administr
DefaultAccount	Utilisateur	Compte utilisateur géré par le sy

243 élément(s) trouvé(s)

ns : Tout Acti Parcc

Tout Active Directory

sio local

- Ce sont les noms qui ont un compte utilisateur du système.

## Postes de la salle :

B18103	Station de travail ou serveur
B18102	Station de travail ou serveur
B181012	Station de travail ou serveur
B181011	Station de travail ou serveur
B181010	Station de travail ou serveur
B18101	Station de travail ou serveur
<b>B181_PROF</b>	<b>Station de travail ou serveur</b>
B181-POSTE2	Station de travail ou serveur
B181-102	Station de travail ou serveur
B18116	Station de travail ou serveur
B18115	Station de travail ou serveur
B1811414	Station de travail ou serveur
B18113	Station de travail ou serveur
B18109	Station de travail ou serveur
B18108	Station de travail ou serveur
B18107	Station de travail ou serveur
B18106	Station de travail ou serveur
B18105	Station de travail ou serveur
B18104	Station de travail ou serveur
B18122	Station de travail ou serveur
B18121	Station de travail ou serveur
B18120	Station de travail ou serveur
B18119	Station de travail ou serveur
B18118	Station de travail ou serveur
B18117	Station de travail ou serveur

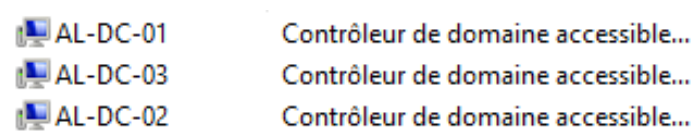
Il n'y a que le poste B181\_PROF qui est sur ETCD, ayant plus de droits que les élèves.

Les autres postes sont sur ETTD.

ETTD (Équipement Terminal de Traitement de Données) permet aux utilisateurs de traiter les données.

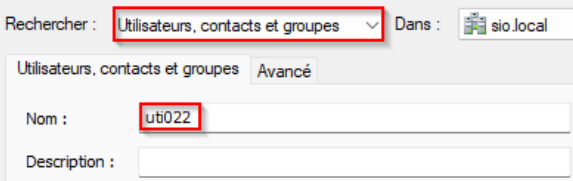
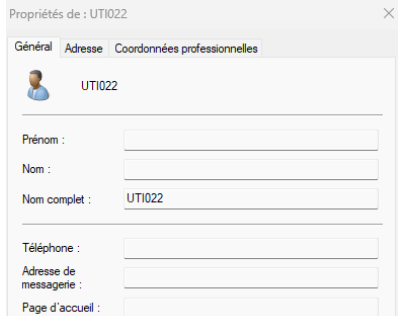
ETCD (Équipement Terminal de Concentration de Données) permet de gérer la transmission des données.

Contrôleurs de domaine :

	<p>On voit une liste des contrôleurs du domaine sio.local. Ils servent la sécurité, l'authentification et les services de nos comptes.</p>
-----------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------

On n'a jamais vu ses noms.

Utilisateur voisin :

	<p>On effectue une recherche des utilisateurs dans le réseau sio.local pour trouver le nom de ma voisine (uti022).</p>
	<p>On n'a pas accès aux informations concernant l'utilisateur, je ne peux donc pas vérifier si c'est bien elle. (Je lui ai demandé son utilisateur pour effectuer une recherche sur elle).</p>

Utilitaire ping et résolution de noms :

Les adresses IP privées sont utilisées essentiellement pour les tests locaux. Elles permettent aux appareils de se connecter et de communiquer entre eux sans être accessibles directement depuis Internet. Ce type d'adresses est très utile pour effectuer des tests en toute sécurité, car elles ne sont pas visibles de l'extérieur.

Ping :

```
C:\Users\uti029>ping 127.25.11.63

Envoi d'une requête 'Ping' 127.25.11.63 avec 32 octets de données :
Réponse de 127.25.11.63 : octets=32 temps<1ms TTL=128
Réponse de 127.25.11.63 : octets=32 temps<1ms TTL=128
Réponse de 127.25.11.63 : octets=32 temps<1ms TTL=128
Réponse de 127.25.11.63 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 127.25.11.63:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\uti029>ping 172.31.1.172

Envoi d'une requête 'Ping' 172.31.1.172 avec 32 octets de données :
Réponse de 172.31.1.172 : octets=32 temps<1ms TTL=128
Réponse de 172.31.1.172 : octets=32 temps<1ms TTL=128
Réponse de 172.31.1.172 : octets=32 temps<1ms TTL=128
Réponse de 172.31.1.172 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 172.31.1.172:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\uti029>ping 127.25.11.65

Envoi d'une requête 'Ping' 127.25.11.65 avec 32 octets de données :
Réponse de 127.25.11.65 : octets=32 temps<1ms TTL=128
Réponse de 127.25.11.65 : octets=32 temps<1ms TTL=128
Réponse de 127.25.11.65 : octets=32 temps<1ms TTL=128
Réponse de 127.25.11.65 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 127.25.11.65:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\uti029>ping 127.25.11.60

Envoi d'une requête 'Ping' 127.25.11.60 avec 32 octets de données :
Réponse de 127.25.11.60 : octets=32 temps<1ms TTL=128
Réponse de 127.25.11.60 : octets=32 temps<1ms TTL=128
Réponse de 127.25.11.60 : octets=32 temps<1ms TTL=128
Réponse de 127.25.11.60 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 127.25.11.60:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

-C'est un protocole ICMP (Internet Control Message Protocol) qui communique des informations sur le réseau et sert principalement à diagnostiquer d'éventuels problèmes.

-Il y a les 3 couches mises en œuvre, la couche 1 et 2 ne sont pas visibles mais permettent de structurer et transporter les paquets et la couche 3 se voit avec l'utilisation de l'ICMP et du ping.

-Les adresses IP privées sont utilisées pour les réseaux privés dans les communications dans ce réseau, afin éviter qu'elles soient attaquables de l'extérieur.

« ping %LOGONSERVER:\=% » :

```
C:\Users\uti029>ping %LOGONSERVER:\=%

Envoi d'une requête 'ping' sur AL-DC-02.sio.local [172.31.1.6] avec 32 octets de données :
Réponse de 172.31.1.6 : octets=32 temps<1ms TTL=128
Réponse de 172.31.1.6 : octets=32 temps<1ms TTL=128
Réponse de 172.31.1.6 : octets=32 temps<1ms TTL=128
Réponse de 172.31.1.6 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 172.31.1.6:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

-L'adresse IP de Shayma est 172.31.1.106 et son nom de poste est B18122.

## 4 : Utiliser Windows PowerShell :

### 4.3 Commandes PowerShell et Invite de commande :

Commande dir :

```
C:\Windows\System32>dir
Le volume dans le lecteur C s'appelle Windows
Le numéro de série du volume est 6867-191D

Répertoire de C:\Windows\System32

17/10/2024 14:05 <DIR> .
01/10/2024 17:38 <DIR> ..
02/10/2024 07:45 <DIR> %userprofile%
07/05/2022 08:01 <DIR> 0409
11/09/2023 21:04 25 960 07489496-a423-4a3e-b620-2cfb0129318d_HyperV-ComputeNetwork.dll
07/05/2022 07:19 25 968 0ae3b980-9a38-4b72-adc4-06849441518d_Servicing-Stack.dll
07/05/2022 07:20 25 952 4545ffe2-0dc4-4df4-9d02-799ef204635e_hvsocket.dll
07/05/2022 07:19 25 952 69fe178f-26e7-43a9-aa7d-2b616b672dde_eventlogservice.dll
30/09/2024 10:52 25 968 6bea57fb-8dfb-4177-9ae8-42e8b3529933_RuntimeDeviceInstall.dll
07/05/2022 07:19 3 176 @AdvancedKeySettingsNotification.png
07/05/2022 07:19 232 @AppHelpToast.png
07/05/2022 07:19 308 @AudioToastIcon.png
07/05/2022 07:19 450 @BackgroundAccessToastIcon.png
07/05/2022 07:19 199 @BitLockerToastImage.png
07/05/2022 07:19 14 791 @edpttoastimage.png
07/05/2022 07:19 330 @EnrollmentToastIcon.png
07/05/2022 07:20 243 815 @facial-recognition-windows-hello.gif
07/05/2022 07:19 563 @language_notification_icon.png
07/05/2022 07:20 699 @optionalfeatures.png
07/05/2022 07:20 354 @StorageSenseToastIcon.png
07/05/2022 07:19 404 @VpnToastIcon.png
07/05/2022 07:20 546 @WindowsHelloFaceToastIcon.png
07/05/2022 07:19 565 @WindowsUpdateToastIcon.contrast-black.png
07/05/2022 07:19 599 @WindowsUpdateToastIcon.contrast-white.png
07/05/2022 07:19 565 @WindowsUpdateToastIcon.png
07/05/2022 07:19 691 @WirelessDisplayToast.png
07/05/2022 07:19 331 @WLO60_96x96.png
30/09/2024 10:52 442 368 aadauthhelper.dll
30/09/2024 14:07 929 792 aadcloudap.dll
30/09/2024 10:52 94 208 aadlcp.dll
30/09/2024 10:51 1 527 296 aadtb.dll
30/09/2024 10:51 226 672 aadWamExtension.dll
30/09/2024 10:51 716 800 AarSvc.dll
30/09/2024 14:08 689 536 AboutSettingsHandlers.dll
30/09/2024 10:52 430 080 AboveLockAppHost.dll
30/09/2024 10:52 294 912 accessibilitycp.dll
30/09/2024 10:53 303 104 accountaccessor.dll
30/09/2024 10:53 491 520 AccountsRt.dll
30/09/2024 10:53 468 456 AcGeneral.dll
30/09/2024 10:53 425 984 Aclayers.dll
07/05/2022 07:20 28 672 acledit.dll
30/09/2024 10:53 569 344 aclui.dll
12/01/2023 10:55 129 984 acm.bin
30/09/2024 14:08 669 056 acmigration.dll
30/09/2024 10:52 249 856 AcPBackgroundManagerPolicy.dll
30/09/2024 10:52 155 648 acppage.dll
07/05/2022 07:20 36 864 acproxy.dll
07/05/2022 07:20 102 400 AcSpecfc.dll
30/09/2024 10:52 401 408 ActionCenter.dll
30/09/2024 10:52 159 744 ActionCenterCPL.dll
07/05/2022 07:19 218 456 ActionQueue.dll
30/09/2024 10:52 196 608 ActivationClient.dll
30/09/2024 14:07 1 019 904 ActivationManager.dll
07/05/2022 07:19 307 200 activeds.dll
```

La commande dir affiche le contenu du répertoire C:\Windows\System32, le volume, le numéro de série du disque et la date de modification de chaque fichier. Elle permet de voir le détail des fichiers et dossiers dans C:\Windows\System32.

Ping	<pre>C:\Windows\System32&gt;ping</pre> <p>utilisation : ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS] [-r count] [-s count] [[-j host-list]   [-k host-list]] [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p] [-4] [-6] nom_cible</p> <p>Options :</p> <ul style="list-style-type: none"> <li>-t Effectue un test ping sur l'hôte spécifié jusqu'à son arrêt. Pour afficher les statistiques et continuer, appuyez sur Ctrl+Attn.</li> <li>-a Pour arrêter, appuyez sur Ctrl+C. Résout les adresses en noms d'hôtes.</li> <li>-n count Nombre de demandes d'écho à envoyer.</li> <li>-l size Taille du tampon d'envoi.</li> <li>-f Active l'indicateur Ne pas fragmenter dans le paquet (IPv4 uniquement).</li> <li>-i TTL Durée de vie.</li> <li>-v TOS Type de service (IPv4 uniquement. La configuration de ce paramètre n'a aucun effet sur le type de service dans l'en-tête IP).</li> <li>-r count Itinéraire d'enregistrement du nombre de sauts (IPv4 uniquement).</li> <li>-s count Horodatage du nombre de sauts (IPv4 uniquement).</li> <li>-j host-list Itinéraire source libre parmi la liste d'hôtes (IPv4 uniquement).</li> <li>-k host-list Itinéraire source strict parmi la liste d'hôtes (IPv4 uniquement).</li> <li>-w timeout Délai d'attente pour chaque réponse, en millisecondes.</li> <li>-R Utilise l'en-tête de routage pour tester également l'itinéraire inverse (IPv6 uniquement). D'après la RFC 5095, l'utilisation de cet en-tête de routage est déconseillée. Certains systèmes peuvent supprimer des demandes d'écho si cet en-tête est utilisé.</li> <li>-S srcaddr Adresse source à utiliser.</li> <li>-c compartment Identificateur de compartiment de routage.</li> <li>-p Effectue un test ping sur l'adresse de fournisseur de la virtualisation réseau Hyper-V.</li> <li>-4 Force l'utilisation d'IPv4.</li> <li>-6 Force l'utilisation d'IPv6.</li> </ul>
Cd	<pre>C:\Windows\System32&gt;cd C:\Users</pre> <pre>C:\Users&gt;</pre> <p>On est passé du répertoire C:\Windows\System32 à C:\Users</p>
Ipconfig	<pre>C:\Windows\System32&gt;ipconfig</pre> <p>Configuration IP de Windows</p> <p>Carte Ethernet Ethernet :</p> <pre> Suffixe DNS propre à la connexion. . . : sio.local Adresse IPv6 de liaison locale. . . . : fe80::dd7c:ed8b:e875:d983%14 Adresse IPv4. . . . . : 172.31.1.172 Masque de sous-réseau. . . . . : 255.255.255.0 Passerelle par défaut. . . . . : 172.31.1.254 </pre>

#### 4.4 : Explorez les applets de commande :

- La commande PowerShell pour dir est « Get-ChildItem ».

#### 4.5 : Commande Netstat avec PowerShell :

## Commande Netsat -h :

```
C:\Windows\System32>netstat -h

Affiche les statistiques de protocole et les connexions réseau TCP/IP actuelles

NETSTAT [-a] [-b] [-e] [-f] [-i] [-n] [-o] [-p proto] [-r] [-s] [-t] [-x] [-y] [interval]

-a           Affiche toutes les connexions et tous les ports d'écoute.
-b           Affiche l'exécutable impliqué dans la création de chaque connexion ou
             port d'écoute. Dans certains cas, des exécutables reconnus hébergent
             plusieurs composants indépendants, et la
             séquence des composants impliqués dans la création de la connexion
             ou du port d'écoute s'affiche alors. Dans ce cas, le
             nom de l'exécutable se trouve dans [] en bas, au-dessus du composant qu'il a appelé,
             et ainsi de suite jusqu'à ce que TCP/IP soit atteint. Notez que cette
             option peut être très longue et qu'elle est susceptible d'échouer si vous n'avez pas
             d'autorisations suffisantes.
-e           Affiche des statistiques Ethernet. Cette option peut être combinée
             avec l'option -s
-f           Affiche les noms de domaine complets (FQDN) pour des adresses
             étrangères.
-i           Affiche le temps passé par une connexion TCP dans son état en cours.
-n           Affiche des adresses et numéros de ports en format numérique.
-o           Affiche l'identificateur du processus propriétaire associé à chaque connexion.
-p proto     Affiche les connexions pour le protocole spécifié par proto ; proto
             peut être l'une des valeurs suivantes : TCP, UDP, TCPv6 ou UDPv6. S'il est utilisé avec l'option -s
             pour afficher les statistiques par protocole, le protocole peut être l'une des valeurs suivantes :
             IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP ou UDPv6.
-q           Affiche toutes les connexions, tous les ports d'écoute et tous les ports
             TCP liés autres que d'écoute. Il se peut que les ports liés autres que les ports d'écoute soient
             ou non associés à une connexion active.
-r           Affiche la table de routage.
-s           Affiche les statistiques par protocole. Par défaut, les statistiques sont affichées pour IP, IPv6, ICMP, ICMPv6, TCP,
             TCPv6, UDP et UDPv6 ; l'option -p peut être utilisée pour
             spécifier un sous-jeu de la valeur par défaut.
-t           Affiche l'état de déchargement de connexion actuel.
-x           Affiche les écouteurs, points de fin partagés et connexions
             NetworkDirect.
-y           Affiche le modèle de connexion TCP pour toutes les connexions.
             Ne peut pas être combiné aux autres options. interval Affiche régulièrement les statistiques sélectionnées, en
             faisant une pause pendant le nombre de secondes spécifié par
             l'intervalle entre chaque affichage. Appuyez sur CTRL+C pour
             arrêter l'affichage des statistiques. Si l'intervalle est omis,
             netstat n'affichera les informations de configuration actuelle qu'une seule fois.
```

- La commande qui permet d'afficher la table de routage de l'ordinateur avec les routes actives est « route print ».

## Route print :

```
C:\Windows\System32>route print

Liste d'Interfaces
14...e0 73 e7 b2 64 d7 .....Intel(R) Ethernet Connection (17) I219-LM
1.....Software Loopback Interface 1

IPv4 Table de routage

Itinéraires actifs :
Destination réseau    Masque réseau    Adr. passerelle    Adr. interface    Métrique
0.0.0.0                0.0.0.0          172.31.1.254       172.31.1.172      25
127.0.0.0              255.0.0.0        On-link            127.0.0.1         331
127.0.0.1              255.255.255.255 On-link            127.0.0.1         331
127.255.255.255        255.255.255.255 On-link            127.0.0.1         331
172.31.1.0             255.255.255.0    On-link            172.31.1.172      281
172.31.1.172           255.255.255.255 On-link            172.31.1.172      281
172.31.1.255           255.255.255.255 On-link            172.31.1.172      281
224.0.0.0              240.0.0.0        On-link            127.0.0.1         331
255.255.255.255        255.255.255.255 On-link            127.0.0.1         331
255.255.255.255        255.255.255.255 On-link            172.31.1.172      281

Itinéraires persistants :
Aucun

IPv6 Table de routage

Itinéraires actifs :
If Metric Network Destination Gateway
1 331 ::1/128 On-link
14 281 fe80::/64 On-link
14 281 fe80::dd7c:ed8b:e875:d983/128 On-link
1 331 ff00::/8 On-link
14 281 ff00::/8 On-link

Itinéraires persistants :
Aucun
```

Nous voyons

La liste des interfaces, Ethernet Intel I219-LM et Software Loopback Interface,

La table de routage IPv4 avec les itinéraires actifs

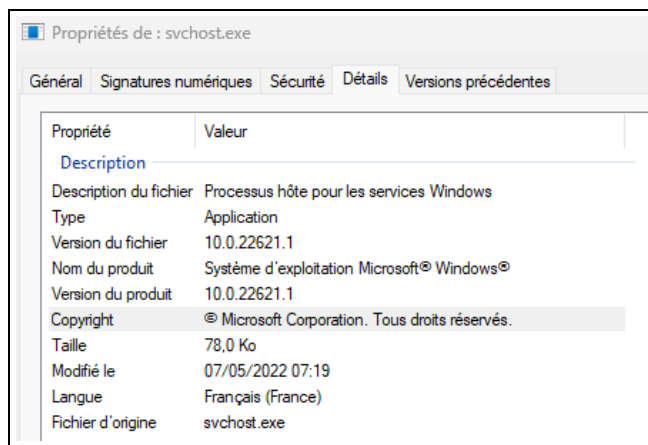
Des exemples d'entrée,

La table de routage IPv6 et

Les itinéraires persistants.

- La passerelle IPv4 est un routeur qui dirige le trafic vers d'autres réseaux quand la destination n'est pas sur le même réseau.

## Informations PID :



PID (Process Identifier) est un identifiant unique pour les processeurs qui sert à suivre et gérer chaque processeur.

#### 4.6 Videz la corbeille avec PowerShell :

- Grâce à la commande « Clear-RecycleBin » sur PowerShell, la poubelle est vidée.

Programme pour afficher les processus actifs et les backdoor existants :

Id	ProcessName	CPU	StartTime
18048	Br-uxendm	272,59375	18/10/2024 14:08:04
18536	msedge	188,734375	18/10/2024 14:08:13
19552	msedge	187,71875	18/10/2024 14:12:40
1180	explorer	88,875	18/10/2024 14:08:01
13916	WINWORD	69,109375	18/10/2024 14:11:27
2316	explorer	61,640625	18/10/2024 14:17:54
1228	msedge	33,96875	18/10/2024 14:08:13
7500	BrHostSvr	14	18/10/2024 14:08:01
18560	msedge	13,4375	18/10/2024 14:08:13
18144	HP.ContextAware	11,234375	18/10/2024 14:08:06
13600	SearchHost	10,515625	18/10/2024 14:08:02
16848	powershell	8,375	18/10/2024 17:00:09
14476	Greenshot	8,25	18/10/2024 14:08:12
20772	msedge	5,90625	18/10/2024 14:13:20
17624	msedgeview2	5,71875	18/10/2024 14:10:03
20496	msedgeview2	3,796875	18/10/2024 14:08:17
6264	ctfmon	3,03125	18/10/2024 14:08:04
14456	msedgeview2	2,765625	18/10/2024 14:10:03
5944	HP.ClientSecurityManager	2,640625	18/10/2024 14:08:01
20292	msedgeview2	2,578125	18/10/2024 14:08:17
19984	msedgeview2	2,171875	18/10/2024 14:08:17
21676	WindowsTerminal	2,03125	18/10/2024 17:00:09
6116	svchost	1,984375	18/10/2024 14:08:01
2904	sihost	1,9375	18/10/2024 14:08:01
21192	msedgeview2	1,8125	18/10/2024 14:10:03
19852	msedgeview2	1,765625	18/10/2024 14:10:03
19612	OneDrive	1,671875	18/10/2024 14:08:15
18220	BrConsole	1,609375	18/10/2024 14:08:05
13940	StartMenuExperienceHost	1,375	18/10/2024 14:08:02
23060	conhost	1,3125	18/10/2024 16:00:04
2784	Widgets	1,15625	18/10/2024 14:08:02
24052	fvenotify	1,015625	18/10/2024 16:58:43
19992	msteams	1,015625	18/10/2024 14:08:16
3004	RuntimeBroker	0,9375	18/10/2024 14:08:03
2516	Br-uxendm	0,734375	18/10/2024 15:09:55
19276	ShellExperienceHost	0,640625	18/10/2024 14:13:03

Fichier contenant le code pour afficher les processus actifs et les backdoors existants :

Processeur\_actifs\_et\_backdoors.txt



```

PS C:\Users\uti029> # 2. Rechercher des backdoors sur des ports critiques (ex. : 4444, 1337, 8080, etc.)
PS C:\Users\uti029> $backdoorPorts = @(4444, 1337, 8080)
PS C:\Users\uti029> Write-Host "nSearching for potential backdoors on suspicious ports (4444, 1337, 8080)..." -ForegroundColor Red

Searching for potential backdoors on suspicious parts (4444, 1337, 8080)...
PS C:\Users\uti029> $networkConnections = Get-NetTCPConnection | Where-Object { $backdoorPorts -contains $_.LocalPort -and $_.State -eq 'Listen' }
PS C:\Users\uti029> if ($networkConnections) {
>> foreach ($backdoor in $networkConnections) {
>>     $process = Get-Process -Id $backdoor.OwningProcess -ErrorAction SilentlyContinue
>>     if ($process) {
>>         Write-Host "Potential Backdoor Detected! Process: $($process.ProcessName), PID: $($backdoor.OwningProcess), Listening on Port: $($backdoor.LocalPort)" -ForegroundColor Red
>>     }
>> } else {
>>     Write-Host "No suspicious backdoors found on the specified ports." -ForegroundColor Green
>> }
No suspicious backdoors found on the specified ports.

```

Il n'y a donc pas de backdoors suspects

- Je m'attendais à ne pas trouver de backdoors suspects, ce qui est arrivé mais pour améliorer le programme et le rendre plus intéressant, on pourrait analyser tous les ports ouverts et pas seulement les ports 4444, 1337 et 8080.

Explications du programme :

- « Write-Host "Listing active processes..." » : Affiche un message informant l'utilisateur que les processus actifs sont en cours d'énumération.
- « Get-Process » : Récupère la liste de tous les processus en cours d'exécution sur la machine.
- « Select-Object Id, ProcessName, CPU, StartTime » : Sélectionne les informations importantes sur chaque processus.
- « Sort-Object -Property CPU -Descending » : Trie les processus par l'utilisation du CPU, du plus élevé au plus bas.
- « Format-Table -AutoSize » : Formate la sortie sous forme de table.
- « \$backdoorPorts = @(4444, 1337, 8080) » : Déclare une liste de ports considérés comme suspects (4444, 1337, et 8080).
- « Write-Host "Searching for potential backdoors..." -ForegroundColor Red » : Affiche un message en rouge pour indiquer qu'une recherche de backdoors est en cours sur les ports spécifiés.
- « Get-NetTCPConnection » : Récupère toutes les connexions TCP actives sur la machine.
- « Where-Object { \$backdoorPorts -contains \$\_.LocalPort -and \$\_.State -eq 'Listen' } » : Filtre les connexions TCP pour ne garder que celles qui écoutent sur les ports spécifiés (4444, 1337, 8080) et dont l'état est 'Listen' (en attente de connexion).
- « if (\$networkConnections) » : Vérifie s'il existe des connexions réseau suspectes sur les ports spécifiés.

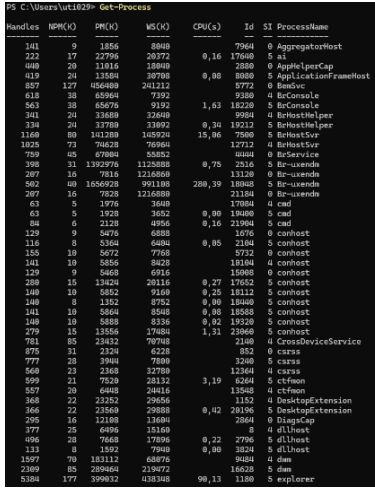
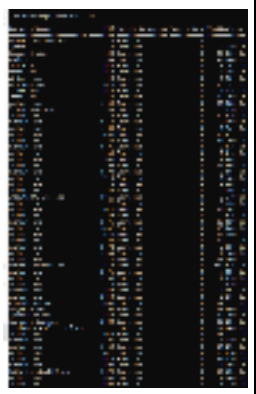
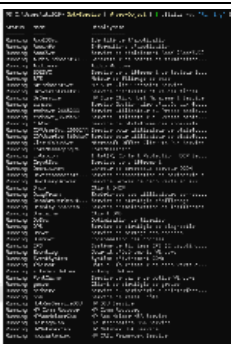




- « foreach (\$backdoor in \$networkConnections) » : Parcourt chaque connexion réseau suspecte.
- « \$process = Get-Process -Id \$backdoor.OwningProcess » : Récupère le processus correspondant à la connexion réseau suspecte en utilisant l'ID du processus propriétaire de la connexion.
- « ErrorAction SilentlyContinue » : ignorer les erreurs si le processus n'est pas trouvé.
- « Write-Host "Potential Backdoor Detected..." » : Si un processus est trouvé, le script affiche un avertissement en rouge, indiquant qu'un backdoor potentiel a été détecté, en fournissant le nom du processus, son PID (Process ID), et le port sur lequel il écoute.
- « else { Write-Host "No suspicious backdoors found..." } » : Si aucune connexion suspecte n'est trouvée, le script affiche un message en vert pour indiquer qu'il n'y a pas de backdoors détectés sur les ports spécifiés.

Commandes pour simplifier les tâches d'un analyste en sécurité :

Get-Process	Récupérer des informations sur les processus qui s'exécutent sur le système. Pour surveiller les processus actifs sur le système
Get-Service   Where-Object { \$_.Status -eq 'Running' }	Lister les services qui sont en cours d'exécution sur le système. Visualiser tous les services en cours d'exécution.
Get-NetTCPConnection	Obtenir des informations détaillées sur les connexions TCP actives sur le système. Afficher des informations détaillées sur les connexions réseau actives.
netstat -an   findstr LISTENING	Lister uniquement les connexions réseau TCP en état "LISTENING" (en écoute). C'est le mélange des commandes netstat -an et findstr LISTENING. Identifier rapidement les ports ouverts.
Get-LocalUser	Lister et récupérer des informations sur les utilisateurs locaux d'un système. Identification des comptes non autorisés ou des comptes créés récemment.

TCP (Transmission Control Protocol) est responsable de la connexion fiable entre deux machines.

Commande PowerShell en ligne de commande :

Get-Process		tasklist	
Get-Service   Where-Object { \$_.Status -eq 'Running' }		sc query state=running	
Get-NetTCPConnection		netstat -ano	
netstat -an   findstr LISTENING		netstat -an   findstr LISTENING	
Get-LocalUser		net user	

## 5: Exercices de calcul de réseaux:

### 5.1: Activité 5:

Adresse IP du serveur 3: 89.0.223.96 car c'est la première du réseau 4

Adresse IP du serveur 2 : 150.179.0.4 car c'est la quatrième du réseau 2

Adresse IP du serveur 1 : 199.64.196.4 car c'est la quatrième du réseau 2

### 5.2 : Activité 6 :

- Le sous-réseau A a besoin de 50 équipements, un masque de /26 pour avoir 64 adresses IP, de 192.168.1.1 à 192.168.1.63, la première et la dernière adresse sont réservées à l'adresse réseau (192.168.1.0) et l'adresse de diffusion (192.168.1.64). Le masque de sous-réseau est 255.255.255.192 car il a potentiellement 64 adresses IP. Le PC A a donc l'adresse IP 192.168.1.1 et l'interface l'adresse IP 192.168.1.62 (la 192.168.1.63 étant déjà prise mais pas sur les interfaces visibles)

```
Router(config-if)#ip address 192.168.1.63 255.255.255.192
Bad mask /26 for address 192.168.1.63

Router#enable
Router#show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/1	unassigned	YES	unset	administratively down	down
GigabitEthernet0/2	unassigned	YES	unset	administratively down	down
Vlan1	unassigned	YES	unset	administratively down	down

L'adresse réseau désigne uniquement le réseau, elle ne peut pas être rattachée à un appareil.

L'adresse de diffusion envoie des messages à tous les appareils du sous-réseau, elle ne peut pas non plus être attribuée à un réseau.

- Le sous-réseau B a besoin de 35 équipements, un masque de /26 permet d'avoir 64 adresses IP, de 192.168.1.66 à 192.168.1.126, la première et la dernière adresse sont réservées à l'adresse réseau (192.168.1.65) et l'adresse de diffusion (192.168.1.127). Le masque de sous-réseau est le même que pour le sous-réseau A (255.255.255.192) car il a le même nombre d'adresses IP possible. L'adresse IP de l'interface sera donc 192.168.1.126 et celle du PC B 192.168.1.66.
- Le réseau C a besoin de 20 équipements, un masque de /27 permet d'avoir 32 adresses IP de 192.168.1.129 à 192.168.1.158, la première et la dernière adresse sont réservées à l'adresse réseau (192.168.1.128) et l'adresse de diffusion (192.168.1.159). le masque de sous-réseau est 255.255.255.224, car il a potentiellement 32 adresses IP. L'interface a donc 192.168.1.126 comme adresse IP et PC C 192.168.1.129
- Le sous-réseau D a besoin de 25 équipements, un masque de /27 permet d'avoir 32 adresses IP de 192.168.1.161 à 192.168.1.189, la première et la dernière adresse sont réservées à l'adresse réseau (192.168.1.160) et l'adresse de

diffusion (192.168.1.191). Le masque de sous-réseau est le même que pour le sous-réseau C (192.168.1.128) car il a le même nombre d'adresses IP possible. L'interface a donc 192.168.1.191 comme adresse IP et PC D 192.168.1.161.

- Le sous-réseau pour la liaison des bâtiments n'a besoin que de 2 adresses IP (pour chaque routeur), un masque de /30 permet d'avoir 4 adresses IP de 192.168.1.193 à 192.168.1.194, la première et la dernière adresse sont réservées à l'adresse réseau (192.168.1.192) et l'adresse de diffusion (192.168.1.195). Le masque de sous-réseau sera de 255.255.255.252 comme il y a maximum 2 adresses IP. L'adresse IP du routeur 1 sera donc 192.168.1.193 et celle du routeur 2 192.168.1.194.

## **Conclusion:**

Ce TP nous a permis de découvrir le protocole TCP/IP, un élément important pour la communication du réseau. Nous avons appris à récupérer des informations réseau, automatiser certaines tâches via PowerShell et effectuer des calculs de sous-réseaux. Ce qui a développé notre capacité à diagnostiquer et administrer un réseau de manière autonome.