Suivi de la connectivité

Protocoles et commandes indispensables

Table des matières

[Introduction : 2](#_Toc184392018)

[1 : Suivi de la connectivité : 2](#_Toc184392019)

[1.1 : Suivre une route vers un serveur distant grâce à Tracert : 2](#_Toc184392020)

[1.1.1 Détermination de la route du trafic internet jusqu’au serveur distant : 2](#_Toc184392021)

[1.1.2 : Interprétation des résultats : 3](#_Toc184392022)

[1.1.3 : Suivi d’une route sur un serveur distant grâce à des outils web et des logiciels : 4](#_Toc184392023)

[1.2 Autres outils d’analyse : 5](#_Toc184392024)

[1.2.1 : Utilisation de la commande pathping : 5](#_Toc184392025)

[1.2.2 : Utilisation de la fonction nslookup : 5](#_Toc184392026)

[1.2.3 : Utilisation de nmap : 7](#_Toc184392027)

[1.2.4 : Utilisation de la fonction route : 17](#_Toc184392028)

[1.2.5 : Utilisation de la fonction netsh : 18](#_Toc184392029)

[1.2.6 : Utilisation de la fonction netstat : 21](#_Toc184392030)

[1.2.7 : Commande net : 24](#_Toc184392031)

[2 : Résolution de problème et suivi de connectivité : 26](#_Toc184392032)

[2.3 : Tester la connectivité de bout en bout avec la commande tracert : 26](#_Toc184392033)

[2.3.1 : Requête ping à partir d’une extrémité du réseau vers l’autre extrémité : 26](#_Toc184392034)

[2.3.2 : Suivez le trafic à partir de PC1 pour de déterminer où se situe le problème de connectivité : 26](#_Toc184392035)

[2.2.3 : Résolution du problème réseau : 27](#_Toc184392036)

[2.4 : Comparer tracert avec traceroute sur un routeur : 29](#_Toc184392037)

[2.5 : Utilisation de la commande extended traceroute : 29](#_Toc184392038)

[2.6 : Ajout d’un routage dynamique : 30](#_Toc184392039)

[Conclusion : 31](#_Toc184392040)

[Sources : 31](#_Toc184392041)

# Introduction :

Dans le domaine des réseaux, la compréhension des outils et des protocoles est essentielle pour garantir une connectivité fiable et efficace. Ce document propose une exploration des principales commandes telles que tracert, pathping ou nmap, afin de permettre aux étudiants d’acquérir des compétences pratiques en suivi et diagnostic des itinéraires empruntés par les données. À travers des exercices ciblés, il s’agit d’apprendre à identifier les problèmes de connectivité, analyser les résultats et mettre en œuvre des solutions adaptées. Cette approche vise à développer une base solide en administration réseau et résolution de problèmes.

# 1 : Suivi de la connectivité :

## 1.1 : Suivre une route vers un serveur distant grâce à Tracert :

### 1.1.1 Détermination de la route du trafic internet jusqu’au serveur distant :

a)

|  |  |
| --- | --- |
|  | Le premier saut est l’adresse IP de la passerelle par default, le second saut est l’adresse IP de notre fournisseur d’accès internet (FAI) et le quatrième et cinquième appartiennent à un fournisseur d’hébergement. Le dernier saut est l’adresse IP de la destination finale. |
|  | Les adresses IP intermédiaires sont juste des étapes.  Les cinq premiers sauts sont toujours les mêmes car il faut que l’adresse IP de destination arrive au FAI, utilise donc toujours le même début. |
|  |  |

b)

|  |  |
| --- | --- |
|  | La RFC 791 établit les directives pour la valeur du champ Time to Live (TTL) dans les paquets IP.  Les RFC sont émises par une organisation qui développe et définit les standards pour Internet, l'Internet Engineering Task Force.  Il y a que les RFC de normes obligatoires qui sont obligatoires, pour l’interopérabilité des systèmes (ex : TCP/IP). |

RFC (Request For Comments) est un document qui spécifie les normes, protocoles et des procédures pour les technologies d’internet.

c)

|  |  |
| --- | --- |
|  | Nombre de sauts est TTL initial -TTL reçu.  La valeur du tableau vide. Il utilise La valeur du système par défaut globale, 128. |
|  | Le TTL reçu est 116.  Le nombre de sauts vaut donc 12. |

### 1.1.2 : Interprétation des résultats :

d)

|  |  |
| --- | --- |
|  | L’adresse IP appartient à RBCI, qui appartient au groupe orange, une FAI. |

e) J’ai utilisé la fonction Whois pour trouver à qui appartient l’adresse IP 81.253.184.86.

f) Les noms de domaine [www.btssio.fr](http://www.btssio.fr) et [www.btssio.org](http://www.btssio.org) n’ont pas été utilisés car ils étaient déjà pris ou sont trop précis pour l’élargissement du site web.

|  |  |
| --- | --- |
|  | Le nom de domaine appartient au lycée Le Castel. |
|  | Il est hébergé par Gandi. |

### 1.1.3 : Suivi d’une route sur un serveur distant grâce à des outils web et des logiciels :

a)

|  |  |
| --- | --- |
| http://ping.eu/ | <http://www.subnetonline.com/pages/network-tools/online-tracepath.php> |
|  |  |

b) Internet utilise un routage dynamique. Les routeurs choisissent le chemin le plus optimal basé sur les conditions actuelles du réseau, il peut y avoir plusieurs meilleurs chemins selon où se base les serveurs des différents sites. De plus selon les régions, les fournisseurs d’accès différents, les routeurs intermédiaires choisis dépendent des points de peering.

Peering est un accord entre deux réseaux pour échanger du trafic gratuitement ou à faible coût, directement entre eux.

c) Asymm (asymmetric routing) indique que le chemin suivi par les paquets pour atteindre une destination n’est pas le même que le chemin suivi par les paquets qui reviennent de cette destination.

Les routeurs utilisent des protocoles pour choisir le chemin le plus optimal selon leurs les coûts, la latence... En cas de surcharge ou de défaillance d’un lien, le chemin aller ou retour peut être aussi rerouté dynamiquement.

## 1.2 Autres outils d’analyse :

### 1.2.1 : Utilisation de la commande pathping :

|  |  |
| --- | --- |
|  | Il y a 3 sauts. |

### 1.2.2 : Utilisation de la fonction nslookup :

|  |  |
| --- | --- |
|  | La commande type permet d’afficher le contenu d’un fichier, ici %windir%\system32\drivers\etc\hosts. |

a)

- Lorsqu’on met une commande ping, le système d’exploitation vérifie dans le fichier host pour voir si le nom existe dedans. S’il n’y est pas, il demande au DNS.

-L’adresse IP de ma voisine (Shayma) est 172.31.1.106.

|  |  |
| --- | --- |
|  | Ouvrir le fichier host |
|  | Je rajoute l’adresse IP et le nom de ma voisine dans le fichier host. Ce fichier associe des noms de domaine à des adresses IP sans passer par le serveur DNS. |
|  | Ping vers Shayma. |

b)

|  |  |
| --- | --- |
|  | On a plus qu’à chercher [www.root-me.org](http://www.root-me.org) pour trouver son temps de conservation. |
|  | Le temps de conservation est de 7153 secondes, 1 heure, 59 minutes et 13 secondes. |

Les résolutions DNS ne sont pas persistantes, elles disparaissent au bout du temps de conservation (TTL) pour laisser la place aux autres. Pour vider son cache, il faut taper la commande « ipconfig /flushdns ».

c)

|  |  |
| --- | --- |
|  | Il permet d’ajouter un nom de domaine et l’adresse IP dans le fichier host. |
|  | Il a bien été ajouté dans le fichier host. |

### 1.2.3 : Utilisation de nmap :

#### 1.2.3.1 : Scan basique d’une machine locale :

|  |  |
| --- | --- |
|  | Les ports ouverts :  135 : msrpc communique entre applications distribuées sur le réseau.  139 : netbios-ssn partage des fichiers et des imprimantes sur des réseaux Windows.  445 : microsoftds partage des fichiers, d'imprimantes et accéder aux ressources sur un réseau Windows.  2179 : vmrdp contrôle à distance des machines virtuelles.  5432 : PostgreSQL gère les connexions client-serveur d’SQL.  16992 : amt-soap-http gère les ordinateurs même lorsqu'ils sont éteints ou hors du système d'exploitation. |

- Le port 22 est la connexion ssh pour les connexions sécurisées, le port 80 est le HTTP pour le transfert des pages web (sans chiffrement) et le port 443 est le HTTPS pour le transfert des pages web mais avec chiffrement.

|  |  |
| --- | --- |
|  | Nmap-f fragmente les paquets, ce qui contourne les IDS/IPS. Certaines ne sont pas capables de les réassembler, la charge de travail augmente aussi, soit elles sont mal analysées soit pas du tout pour aller plus vite. |

- Les IDS et IPS analysent le trafic réseau pour détecter les comportements suspects. L’IDS ne les bloquent pas mais les signale contrairement aux IPS qui les bloquent.

#### 1.2.3.2 : Scanne des ports spécifiques :

|  |
| --- |
|  |

- En limitant les scans à certains ports nous gagnons du temps et de la lisibilité en aillant seulement les ports qui nous intéressent sans regarder tous les autres.

- De plus on diminue l'impact sur la bande passante car scanner trop de ports consomme beaucoup de trafic réseau.

- Un scan intensif peut aussi parfois causer des problèmes aux systèmes scannés, comme des ralentissements ou des pannes de services. Pour éviter au maximum cela, il faut juste scanner les ports qui nous intéresse pour éviter d’endommager des ports inutilement.

- Un scan complet de tous les ports est souvent détecté par les systèmes de détection d'intrusion et les pares-feux. En limitant le nombre de ports scannés, il est possible de rester plus discret et d'éviter d'alerter les systèmes de sécurité.

|  |  |
| --- | --- |
|  | Les services SSH, http et HTTPS sont présents mais fermé car ce sont des ports standards. Ils sont fermés car personne ne les utilise. |

#### Scanne de service et gestion :

|  |  |
| --- | --- |
|  | 135 : un service msrpc et avec une version Windows RPC.  139 : un service netbios-ssn et avec une version Microsoft Windows netbios-ssn.  445 : un service peut être microsoft-ds et avec une version inconnue  2179 : un service peut être vmrdp et avec une version inconnue.  5432 : un service postgresql et avec une version postgreSQL DB.  16992 : un service http et avec une version Intel AMT WebUI 16.1.32.2418 (Standard Manageability). |

- Les versions obsolètes sont souvent connues pour avoir des failles de sécurité qui sont documentées publiquement, ce qui rend le système vulnérable à des attaques exploitant ces failles. Les logiciels obsolètes ne reçoivent plus de mises à jour de sécurité, ce qui expose le système à des menaces récentes sans possibilité de protection. Les anciennes versions peuvent être incompatibles avec des systèmes modernes, augmentant le risque de pannes et de dégradations des performances.

Pour pallier tout ça, il est recommandé de mettre à jour les logiciels pour éviter les services obsolètes et corriger les failles connues. Utiliser des pares-feux pour restreindre l’accès aux ports vulnérables et segmenter le réseau pour isoler les services obsolètes.

#### : Scanne avec détection d’OS :

|  |  |
| --- | --- |
|  | C’est moyennement fiable car il me propose deux OS : Microsoft Windows 10 et Microsoft Windows 11. |

|  |  |
| --- | --- |
|  | Mon poste est sur Windows 11, il est bien dans ce que la commande m’a proposé. |

- Chaque système d'exploitation a des vulnérabilités spécifiques. Si un attaquant connaît l'OS exact, il peut se concentrer sur les exploits connus pour cette plateforme.

Certains services sont souvent préinstallés et activés par défaut selon l'OS. Si un attaquant connaît l'OS, il peut identifier les services vulnérables associés à cet OS et tenter des attaques spécifiques à ces services.

Savoir quel OS est utilisé peut permettre à un attaquant de créer des attaques spécifiquement adaptées.

**-** Une fois l'OS identifié, l'attaquant peut rechercher les vulnérabilités spécifiques à cette version d'OS, ce qui lui permet d’utiliser des exploits existants.

Chaque OS a des services (ports) par défaut qui peuvent être ouverts. Un attaquant peut se concentrer sur ces services, en utilisant des outils (comme Nmap) pour tester la présence de vulnérabilités associées.

La divulgation de l'OS augmente la surface d'attaque en fournissant des indices qui permettent à un attaquant d’adapter ses outils et techniques d'exploitation, de cibler des vulnérabilités spécifiques à la version de l’OS. Pour minimiser ses risques, on doit désactiver la divulgation d’informations sur l’OS et ne pas laissez de services inutiles actifs.

#### 1.2.3.5 : Scanne en mode furtif :

|  |  |
| --- | --- |
|  | Il y a juste le temps de latence qui est 3 fois moins élevée sur un scan furtif par rapport à un scan standard. |
|  |  |

- Ce type de scanne est souvent utiliser car il permet aux attaquants de moins se faire détecter et aux administrateurs de sécurité d’être plus rapide sans perturber les services existants.

- Le scan SYN n’établit pas complètement la connexion, elle envoie un paquet SYN (synchronisation) pour établir une connexion TCP et le scanner renvoi un paquet RST (reset) pour fermer la connexion. Le scan complet quant à lui reçoit un paquet ACK (accusé de réception), la connexion est ouverte et il peut donc envoyer des données.

Le scan SYN est donc moins repérable, il génère moins de trafic réseau, perturbe moins le fonctionnement des services et réduit la consommation de ressources.

Le scan complet est détectable facilement, utilise plus de ressources et est plus lents mais fournit plus d’informations.

- Le scan SYN a un moins grand impact sur les logs (journaux du système) car il a une réponse RST qui limite la connexion et donc les informations collectées. Il est aussi moins repérable, donc moins d’informations dessus.

Le scan complet a accès aux informations complètes comme l’adresse IP source et de destination par exemple et est identifier clairement sur le réseau. Il a un plus grand impact sur les logs, ça dépend du scan en lui-même.

Un log est un journal du système qui enregistre des événements liés au fonctionnement du système d'exploitation. Il est utile pour suivre l’activité du système, analyser les problèmes, et assurer la sécurité des systèmes informatiques.

#### 1.2.3.6 : Analyse de vulnérabilité :

|  |  |
| --- | --- |
|  | Il n’y a pas de vulnérabilité détectée. |

- pour résoudre des problèmes, on peut mettre à jour Windows pour que les mises à jour de sécurité soient appliquées, désactiver SMBv1, car elle est obsolète. On peut aussi désactiver Avahi si on n’a pas besoin de découvrir le réseau.

- Nessus et Open Vas maintiennent une base de données constamment mise à jour avec des vulnérabilités connues dedans. Ça leur permet de tester les systèmes à la recherche de vulnérabilités spécifiques. Ils comparent aussi les services et les versions des logiciels trouvés sur le système avec cette base de données pour identifier les vulnérabilités potentielles. Ils font aussi un scan réseau, comme celui d’Nmap, pour identifier les ports ouverts et les services correspondants. Ils simulent aussi des attaques pour trouver des failles et vérifient les configurations des systèmes pour s'assurer qu'elles respectent les bonnes pratiques de sécurité. Ils font un rapport détailler avec la gravité de chaque risque.

Qualys est basé sur le cloud, on peut donc faire des scans à grande échelle.Il planifie des analyses de vulnérabilité de manière automatisée, surveille en temps réel, garanti la conformité avec les normes de sécurité et propose des solutions pour corriger les vulnérabilités.

#### 1.2.3.7 : Trouver une vulnérabilité :

On n’a pas trouvé de failles visibles avec la commande netsh, on va utiliser des commandes plus avancées et Linux pour en trouver.

|  |  |
| --- | --- |
| Une image contenant texte, capture d’écran, Police, noir et blanc  Description générée automatiquement | On commence par scanner pour voir tous les appareils du réseau (-sL). |
| Une image contenant texte, capture d’écran, Police, noir et blanc  Description générée automatiquement | Ou si l’on veut voir les hôtes les plus « bruyant » ce qui émettent le plus de trame en ce moment (-sn). |

##### 1.2.3.7.1 : Nous allons au hasard analyser deux adresses ip du réseau :

|  |
| --- |
| Une image contenant texte, capture d’écran, Police  Description générée automatiquement |

Et celle si que nous avons vue dans le -sL :

|  |
| --- |
| Une image contenant texte, capture d’écran, Police  Description générée automatiquement |

Celle-ci a été choisie délibérément server wsus indique que c’est un server de déploiement d’image /mise à jour il serait donc critique qu’un tel e system sois sensible.

Un serveur de déploiement d’image/mise à jour est utilisée pour gérer et distribuer des images système et des mises à jour logicielles vers les appareils dans un réseau. Il créé des images standardisées du système d’exploitation pouvant être envoyées sur plusieurs machines simultanément. Il gère aussi la distribution des correctifs de sécurité et des mises à jour logicielles. Il est donc primordial de le mettre à jour pour qu’il puisse faire les correctifs de sécurité et les mises à jour les plus récentes.

##### 1.2.3.7.2 : Installation de métasplot :

Sous linux Ubuntu :

|  |  |
| --- | --- |
| Une image contenant texte, capture d’écran, Police  Description générée automatiquement | sudo apt update  sudo apt upgrade -y |

git clone https://github.com/offensive-security/exploitdb.git /opt/exploitdb :

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Une image contenant texte, Police, capture d’écran, ligne

Description générée automatiquement

##### 1.2.3.7.3 : Analyse de l’active directory :

Maintenant que l’on a analyser que l’active directory avais une version service http lier au service RCP :

Une image contenant texte, capture d’écran, Police, ligne

Description générée automatiquement

Chaque liste que vous voyer ici est une faille de sécurité public et connue répertorier sur exploit db, il serais important d’effectuer les mise à jour car ce sont de simples failles de sécurité que l’on peut corriger facilement.

##### 1.2.3.7.4 : Analyse Wsus :

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

|  |  |
| --- | --- |
| Une image contenant texte, capture d’écran, Police  Description générée automatiquement | On voit toutes les failles de l’httpd 2.0 en rouge |
|  |  |

Une image contenant texte, capture d’écran, menu, Police

Description générée automatiquement

#### 1.2.3.8 : Faire un script pour automatiser nmap :

Structure du Fichieranalyse.bat :

- Mon fichier analyse.bat contient la ligne de commande suivante :

Une image contenant texte, capture d’écran, Police, ligne

Description générée automatiquement

Étapes de l'Automatisation :

Préparation de la Liste des Adresses IP (liste.txt) :

J'ai créé un fichier nommé liste.txt où je liste toutes les adresses IP de mon réseau que je souhaite scanner. Chaque adresse IP est inscrite sur une nouvelle ligne :

Une image contenant texte, capture d’écran, logiciel, nombre

Description générée automatiquement

Cela permet de centraliser toutes les cibles de scan dans un seul fichier, ce qui facilite la gestion et la mise à jour des adresses à scanner.

Cette commande permet à Nmap de lire les adresses IP depuis liste.txt grâce à l'option -iL et d'activer la détection des versions des services avec -sV. Les résultats du scan sont ensuite ajoutés au fichier log-nmap-.txt sans effacer les précédents grâce à l'opérateur >>. Cela me permet de conserver un historique complet des analyses effectuées.

- Pour automatiser le processus, j'exécute simplement le fichier analyse.bat. Chaque exécution lance Nmap, qui scanne les adresses listées et enregistre les résultats dans le fichier de log. Pour une automatisation complète, j'utilise le Planificateur de tâches Windows. Cela me permet de programmer l'exécution régulière du script ce qui assure les scans fréquents sans intervention manuelle.

La gestion des logs est facilitée par cette automatisation. Le fichier log-nmap-.txt accumule les résultats de chaque scan, ce qui me permet de suivre l'évolution du réseau et de détecter rapidement toute anomalie ou changement, comme des ports ouverts inattendus ou des versions de services obsolètes. En surveillant régulièrement ce fichier, je peux renforcer la sécurité de mon réseau en prenant des mesures correctives lorsque nécessaire.

1.2.4 : Utilisation de la fonction route :

a) La commande route gère la route qui va être emprunter par les paquets, on peut donc configurer par ou elle va passer et l’afficher.

b)

|  |  |
| --- | --- |
|  | C’est l’adresse de l’itinéraire par default, tout ce qui sort du réseau passera par la passerelle 172.31.1.254. |

c) C’est l’adresse de bouclage, tout ce qui est destiné à ce réseau passe par ce poste. C’est utilisé principalement pour des tests locaux.

d) 172.31.1.0 c’est l’adresse de réseau, la plus basse du sous-réseau. Elle est utilisée pour identifier ce sous-réseau. Elle ne peut pas être attribuée à un hôte.

e) L'adresse IPv6 de loopback est ::1. C'est l'équivalent de 127.0.0.1 en IPv4, utilisée pour les communications internes à la machine, c'est-à-dire pour tester la pile TCP/IP du système sans avoir besoin de connexion réseau physique.

|  |  |
| --- | --- |
| Une image contenant texte, capture d’écran, logiciel  Description générée automatiquement | La première ligne |

Loopback est une interface réseau virtuelle qui permet à un appareil de communiquer avec lui-même. Elle n'implique aucune communication réelle sur un réseau physique externe.

### 1.2.5 : Utilisation de la fonction netsh :

#### 1.2.5.1 : Exercice de découverte :

a)

|  |  |
| --- | --- |
|  | On voit l’identifiant de l’interface (Idx), la métrique de l’interface (Mét), la taille maximale de transfert unitaire (MTU), l’état de l’interface et son nom |

La métrique sert à déterminer la priorité des routes. Plus elle est basse, plus c’est une priorité dans le routage.

b)

|  |  |
| --- | --- |
|  | - netsh pour lancer l'outil en ligne de commande de configuration réseau.  - Interface pour spécifier que l'on travaille sur des interfaces réseau.  Show interface pour Affiche toutes les interfaces réseau disponibles sur le système avec leur état. |

|  |  |
| --- | --- |
|  | Ipv6 pour indiquer que l'on va travailler avec la configuration IPv6 des interfaces.  Show neighbors pour afficher tous les voisins IPv6 que la machine a rencontrés. |

c)

|  |  |
| --- | --- |
|  | Int ip pour indiquer que l'on souhaite travailler sur la pile IP.  Rest pour réinitialiser aux valeurs par default. |

Il faut redémarrer le poste pour que les modifications de la commande soit pris en compte.

d) Le poste est en communication avec toute les connexions TCP « Etabli », donc avec 51.178.91.234, le port 6568, avec 40.74.219.49 le port 443 (HTTPS), avec 20.199.120.85 le port 443 (HTTPS), avec 52.42.216.19 le port 443 (HTTPS) et avec 64.91.226.82 le port 443 (HTTPS).

e) Les toutes les adresses IP externes doivent être examinées pour vérifier qu’elles soient bien des services ou des sites légitimes. Surveiller le nombre de connexions locales, si elles sont inhabituelles, des logiciels malveillants peuvent s'injecter dans des processus locaux ou d'établir des communications avec d'autres processus internes. Laisser des ports ouverts inutilement expose l'ordinateur à des attaques potentielles, il faut donc fermer ceux qui sont inutile.

#### 1.2.5.2 : Sauvegarder et restaurer la configuration réseau :

Cette fonctionnalité est particulièrement utile pour une récupération rapide après un incident réseau. C’est un gain de temps. Lorsqu'un administrateur doit déployer la même configuration réseau sur plusieurs machines, ça peut être très longs. Avec la commande netsh, l'administrateur peut générer un fichier de configuration à partir d'une machine correctement configurée, puis appliquer cette même configuration sur d'autres postes. Lors de la migration de configurations réseau vers de nouveaux appareils. Plutôt que de tout reconfigurer manuellement sur le nouvel appareil, l'administrateur, il applique le même script de configuration.

|  |
| --- |
|  |

#### 1.2.5.3 : Configurer les règles de pare-feu avec netsh :

Il faut exécuter l’invite de commande en mode administrateur car les commandes autoriser Chrome et bloquer FTP modifient des paramètres de sécurité (Dans le pare-feu Windows).

|  |
| --- |
|  |
|  |
|  |
|  |

Les règles sont bien appliquées.

- Un pare-feu restreint ou permet d’accéder à des applications en fonctions des regels de sécurité définies. Il filtre le trafic au niveau de la couche application (couche 7) en identifiant le type d’application qu’utilise le réseau. Il est aussi capable de reconnaitre des processus spécifiques sur un système et de bloquer ce trafic pour limiter la propagation de logiciels malveillants et de réduire les risques d’intrusions. Il contrôle aussi les applications en fonction du groupe d’utilisateurs (ou de l’utilisateur) et peut restreindre les applications ou ports avec des règles granulaires, autorisation seulement en semaine de 8h jusqu’à 18h par exemple. Il peut aussi fermer les ports ouverts inutilisés, autoriser le trafic que sur des ports spécifiques et masquer les ports fermés pour donner moins d’informations lors un scan de ports par des hackeurs. Il suit la connexion au réseau séparant le trafic légitime du trafic non sollicité.

|  |
| --- |
|  |

### 1.2.6 : Utilisation de la fonction netstat :

a)

|  |  |
| --- | --- |
|  | Il y a que les ports TCP activés. |

b)

|  |  |
| --- | --- |
|  | La carte Ethernet marche bien car il n’y a pas de rejets ni d’erreurs ni de protocoles inconnus. |

c)

|  |  |
| --- | --- |
|  | Le procole le plus utilisé est l’IPv4 |
|  |  |
|  |  |

d)

|  |  |
| --- | --- |
| Une image contenant texte, capture d’écran, menu  Description générée automatiquement | netstat -abno |

D'après l'échantillon de ma sortie de la commande netstat -abno, j'ai identifié plusieurs fichiers exécutables impliqués dans la création des connexions réseau sur mon ordinateur. Parmi ces exécutables, il y a svchost.exe, qui héberge plusieurs services Windows essentiels. J'ai remarqué LMS.exe, associé au service de gestion des licences, ainsi que vmms.exe, responsable du gestionnaire de machines virtuelles utilisé par Hyper-V. Le processus postgres.exe indique l'utilisation de la base de données PostgreSQL, tandis que spoolsv.exe gère les tâches d'impression.

J'ai également identifié des applications utilisateur telles que msedge.exe pour le navigateur Microsoft Edge, OneDrive.exe pour la synchronisation des fichiers avec OneDrive, et ChatGPT.exe, qui semble être une application spécifique installée sur mon système.

e) J’ai répondu à ça dans la D. Les PID sont à droite des noms dans ma capture CMD et l’on peut les éteindre directement avec un taskkill. Certains PID (PID 4) n'ont pas pu être associés à un nom d'exécutable spécifique car ce sont des processus système protégés comme que le processus System.

### 1.2.7 : Commande net :

a)

|  |  |
| --- | --- |
|  | C$ est un partage administratif de la partition C:\, pour avoir accès à la racine du disque à distance.  D$ est similaire à C$ mias avec le disque D:\.  IPC$ établit une connexion inter-processus entre deux machines sur un réseau.  print$ ajouter ou gérer des imprimantes sur un réseau.  admin$ donne accès au répertoire C:\windows. |

b)

La commande net computer est principalement utilisée pour ajouter ou supprimer des comptes d'ordinateurs dans un domaine Active Directory.

|  |  |
| --- | --- |
|  |  |
|  | Afficher les ressources partagées d’un ordinateur ou d’un serveur spécifique. |
|  | Il n’y a pas de ressoucres partagées dans mon ordinateur. |

c)

|  |  |
| --- | --- |
|  |  |
|  | Pour afficher des informations sur la configuration du poste. |

|  |  |
| --- | --- |
| Net session |  |
| Net session \\nom\_ordinateur |  |
| Net start service |  |
| Net stop service |  |

# 2 : Résolution de problème et suivi de connectivité :

## 2.3 : Tester la connectivité de bout en bout avec la commande tracert :

### 2.3.1 : Requête ping à partir d’une extrémité du réseau vers l’autre extrémité :

|  |  |
| --- | --- |
|  | Le ping n’a pas fonctionné, tous les paquets se sont perdus. Il y a donc un problème de connectivité |

### 2.3.2 : Suivez le trafic à partir de PC1 pour de déterminer où se situe le problème de connectivité :

|  |  |
| --- | --- |
|  | La premier adresse IP 10.0.0.254 appartient à GigabitEthernet 0/0 |
|  | L’interface GigabitEthernet 0/0 représentent des ports physiques par lesquels le périphérique est connecté à d'autres appareils du réseau. |

|  |  |
| --- | --- |
|  | La dernière adresse IP est 10.100.100.6, celle du routeur C |

### 2.2.3 : Résolution du problème réseau :

a) Le router B, le router C et le router D on des adresses entourant la dernière de la commande tracert : 10.100.100.4<1.100.100.6<1.100.100.8.

b)

|  |  |
| --- | --- |
|  | Les interfaces sont actives. |

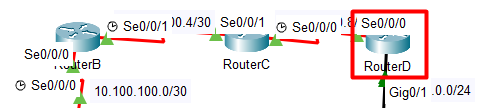
|  |
| --- |
|  |

J’ai utilisé l’enveloppe ICMP pour détecter l’endroit ou l’enveloppe ne peut plus passer. Je trouve ça plus visuel et avec le PDU on a plus d’informations.

|  |  |
| --- | --- |
|  | La table CEF ne contient pas d'entrée pour l'adresse IP de destination. Ce qui force le routeur à consulter la table de routage traditionnelle. Mais la table de routage ne contient pas la route. Il est donc incapable d’acheminer le paquet. |

CEF est conçu pour accélérer le processus de transfert des paquets en fournissant un accès rapide aux informations de routage pré-calculées.

c)



Commande show running-config (pour voir les adresses IP et les masques de sous-réseau) :

|  |  |
| --- | --- |
|  | Les masques de sous-réseau Serials (les câbles utilisés) sont bons.  L’adresse IP de Serial0/0/0 n’est pas bonne, comme elle est reliée au routerD. |

d) Il faut attribuer l’adresse IP mis dans la topologie sur le routerD:

|  |  |
| --- | --- |
|  | 10.100.100.9 au lieu de  10.100.100.17 |

|  |  |
| --- | --- |
|  | La commande tracert et l’enveloppe ICMP marchent et arrivent au PC3 |
|  |  |

## 2.4 : Comparer tracert avec traceroute sur un routeur :

|  |  |
| --- | --- |
|  | Ca fonctionne bien car la dernière adresse est celle de PC3. |
|  |  |

Il y a le premier saut qui est différent, celui du PC1, la d’où commence la trame.

## 2.5 : Utilisation de la commande extended traceroute :

a)

|  |  |
| --- | --- |
|  | La commande extended traceroute, entrée dans le mode privilégié n’est pas reconnu. Il faut juste utiliser la commande traceroute dans le mode privilégié. |
|  | Trois réponses sont personnalisées :  Target IP address : 10.1.0.2  Source address : 10.100.100.1  Probe count : 5 (au lieu de 3) |

b)

|  |  |
| --- | --- |
|  | 5 paquets ICMP sont envoyés à chaque saut, comme défini (Probe count). Routeur A a envoyé 5\*4, donc 20 paquets. |

c)

|  |  |
| --- | --- |
|  | Le router va attendre 4 secondes de plus les réponses ICMP. |

d) Il y a plus de réponses car plus de temps pour répondre si un routeur est surchargé ou lent mais plus de temps d’attente des résultats par celui qui a tapé la commande. Il permet aussi de déterminer si c’est une latence excessive plutôt qu’a une défaillance complète.

## 2.6 : Ajout d’un routage dynamique :

Le routage dynamique utilise des protocoles pour ajuster automatiquement les itinéraires dans un réseau. Le routage est en mode statique avec les configurations manuelles des routes statiques (ip route <réseau distant> <masque réseau réseau distant> <passerelle d'accès>). Nous utiliserons le protocole rip2 car il est adapté aux petits réseaux et est chiffré.

Configuration des routeurs :

|  |  |
| --- | --- |
|  | 3 : activer le processus de routage RIP.  4 : définit la version de RIP à utiliser (le RIP1 est par default)  5 : activer le routage pour le réseau 10.0.0.0  6 : activer le routage pour le réseau 10.100.100.0 |

Les commandes en grises sont a remplacer par les adresses correspondantes :

|  |  |  |  |
| --- | --- | --- | --- |
| Router : | Network 1 | Network 2 | Network 3 |
| Router A | 10.0.0.0 | 10.100.100.0 |  |
| Router B | 10.100.100.0 | 10.100.100.4 | 10.1.0.0 |
| Router C | 10.100.100.4 | 10.100.100.8 | 10.1.0.0 |
| Router D | 10.1.0.0 | 10.100.100.8 |  |

Les adresses utilisées sont celles des interfaces voisines des routeurs.

Vérification :

|  |
| --- |
|  |

# Conclusion :

Ce TP nous a permis de nous plonger dans des situations concrètes de gestion et de dépannage réseau. Nous avons analysé et la gérer des réseaux, et anticiper et réagi rapidement face à des problèmes de connectivité. Il nous a montré brièvement comment étaient les métiers d’administrateurs réseau et de professionnels en sécurité informatique où la maîtrise de ces outils est essentielle pour assurer une infrastructure fonctionnelle et sécurisée.

# Sources :

https://www.it-connect.fr/ajouter-une-route-statique-sur-un-routeur-cisco%EF%BB%BF/

[Comprendre les commandes Ping et Traceroute étendues - Cisco](https://www.cisco.com/c/fr_ca/support/docs/ip/routing-information-protocol-rip/13730-ext-ping-trace.html)

[Loopback — Wikipédia](https://fr.wikipedia.org/wiki/Loopback)