

# SUIVI DE LA CONNECTIVITE

Protocoles et commandes indispensables

## Table des matières

Introduction : .....	2
1 : Suivi de la connectivité : .....	2
1.1 : Suivre une route vers un serveur distant grâce à Tracert : .....	2
1.1.1 Détermination de la route du trafic internet jusqu'au serveur distant : .....	2
1.1.2 : Interprétation des résultats : .....	3
1.1.3 : Suivi d'une route sur un serveur distant grâce à des outils web et des logiciels : .....	4
1.2 Autres outils d'analyse : .....	5
1.2.1 : Utilisation de la commande pathping : .....	5
1.2.2 : Utilisation de la fonction nslookup : .....	5
1.2.3 : Utilisation de nmap : .....	7
1.2.4 : Utilisation de la fonction route : .....	17
1.2.5 : Utilisation de la fonction netsh : .....	18
1.2.6 : Utilisation de la fonction netstat : .....	21
1.2.7 : Commande net : .....	24
2 : Résolution de problème et suivi de connectivité : .....	26
2.3 : Tester la connectivité de bout en bout avec la commande tracert : .....	26
2.3.1 : Requête ping à partir d'une extrémité du réseau vers l'autre extrémité : ....	26
2.3.2 : Suivez le trafic à partir de PC1 pour de déterminer où se situe le problème de connectivité : .....	26
2.2.3 : Résolution du problème réseau : .....	27
2.4 : Comparer tracert avec traceroute sur un routeur : .....	29
2.5 : Utilisation de la commande extended traceroute : .....	29
2.6 : Ajout d'un routage dynamique : .....	30
Conclusion : .....	31
Sources : .....	31

## 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)

<pre>C:\Users\uti029&gt;tracert -d peugeot.fr  Détermination de l'itinéraire vers peugeot.fr [217.70.184.55] avec un maximum de 30 sauts :   1  &lt;1 ms  &lt;1 ms  &lt;1 ms  172.31.1.254  2  &lt;1 ms  &lt;1 ms  &lt;1 ms  100.100.1.160  3  &lt;1 ms  1 ms   &lt;1 ms  46.18.224.51  4  2 ms   2 ms   2 ms   85.31.197.93  5  3 ms   3 ms   3 ms   85.31.197.92  6  8 ms   8 ms   8 ms   195.234.35.69  7  8 ms   8 ms   8 ms   37.49.237.108  8  8 ms   8 ms   8 ms   100.99.1.89  9  8 ms   9 ms   19 ms  100.99.0.19 10  8 ms   8 ms   8 ms   100.100.0.229 11  8 ms   8 ms   8 ms   173.246.102.3 12  8 ms   8 ms   8 ms   173.246.102.5 13  8 ms   8 ms   8 ms   10.12.0.6 14  8 ms   8 ms   8 ms   217.70.184.55  Itinéraire déterminé.</pre>	<p>Le premier saut est l'adresse IP de la passerelle par défaut, 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.</p>
<pre>C:\Users\uti029&gt;tracert -d sfr.fr  Détermination de l'itinéraire vers sfr.fr [80.125.163.172] avec un maximum de 30 sauts :   1  &lt;1 ms  &lt;1 ms  &lt;1 ms  172.31.1.254  2  &lt;1 ms  &lt;1 ms  &lt;1 ms  100.100.1.160  3  &lt;1 ms  &lt;1 ms  &lt;1 ms  46.18.224.51  4  2 ms   2 ms   2 ms   85.31.197.93  5  3 ms   2 ms   2 ms   85.31.197.92  6  3 ms   2 ms   2 ms   85.31.194.149  7  7 ms   7 ms   7 ms   77.95.71.13  8  10 ms  10 ms  10 ms   194.6.146.53  9  9 ms   10 ms  9 ms   194.6.146.53 10  8 ms   9 ms   8 ms   109.6.13.202 11  *      *      *      Délai d'attente de la demande dépassé. 12  9 ms   9 ms   9 ms   80.125.163.172  Itinéraire déterminé.</pre>	<p>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.</p>
<pre>C:\Users\uti029&gt;tracert -d cisco.fr  Détermination de l'itinéraire vers cisco.fr [72.163.4.154] avec un maximum de 30 sauts :   1  &lt;1 ms  &lt;1 ms  &lt;1 ms  172.31.1.254  2  &lt;1 ms  &lt;1 ms  &lt;1 ms  100.100.1.160  3  1 ms   1 ms   &lt;1 ms  46.18.224.51  4  3 ms   2 ms   2 ms   85.31.197.93  5  2 ms   2 ms   3 ms   85.31.197.92  6  124 ms 124 ms 124 ms  72.163.4.154  Itinéraire déterminé.</pre>	

b)

Internet Protocol Datagram		RFC791	
Source	Destination	Version	<input type="checkbox"/> If other than version 4, attach form RFC 2460.
<b>Type of Service</b> <input type="checkbox"/> reliable <input type="checkbox"/> low delay <input type="checkbox"/> high throughput	<b>Precedence</b> <input type="checkbox"/> Routine <input type="checkbox"/> Priority <input type="checkbox"/> Immediate <input type="checkbox"/> Flash <input type="checkbox"/> Flash Override <input type="checkbox"/> CRITIC/ECP <input type="checkbox"/> Internetwork Control <input type="checkbox"/> Network Control	<b>Fragmentation</b> Transport layer use only <input type="checkbox"/> more to follow <input type="checkbox"/> do not fragment <input type="checkbox"/> this bit intentionally left blank	<b>Offset</b> <input type="text"/>
<b>Protocol</b> <input type="checkbox"/> TCP <input type="checkbox"/> UDP <input type="checkbox"/> Other	<b>Length</b> <input type="text"/> <b>Header Length</b> <input type="text"/>	<b>Data</b> Print legibly and press hard. You are making up to 255 copies.	
<b>Time to Live</b> <input type="text"/>	<b>Options</b> Do not write in this space.	<b>Header Checksum</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)

<pre>PS C:\Users\uti029&gt; Get-NetIPInterface   Select-Object DefaultTTL DefaultTTL ----- 128</pre>	<p>Nombre de sauts est TTL initial -TTL reçu.</p> <p>La valeur du tableau vide. Il utilise La valeur du système par défaut globale, 128.</p>
<pre>C:\Users\uti029&gt; ping 8.8.8.8  Envoi d'une requête 'Ping' 8.8.8.8 avec 32 octets de données : Réponse de 8.8.8.8 : octets=32 temps=8 ms TTL=116 Réponse de 8.8.8.8 : octets=32 temps=8 ms TTL=116 Réponse de 8.8.8.8 : octets=32 temps=8 ms TTL=116 Réponse de 8.8.8.8 : octets=32 temps=8 ms TTL=116  Statistiques Ping pour 8.8.8.8:     Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),     Durée approximative des boucles en millisecondes :         Minimum = 8ms, Maximum = 8ms, Moyenne = 8ms</pre>	<p>Le TTL reçu est 116.</p> <p>Le nombre de sauts vaut donc 12.</p>

### 1.1.2 : Interprétation des résultats :

d)

<pre>Whois IP 81.253.184.86  % This is the RIPE Database query service. % The objects are in RPSL format. % % The RIPE Database is subject to Terms and Conditions. % See https://docs.db.ripe.net/terms-conditions.html % % Note: this output has been filtered. % To receive output for a database update, use the "-b" flag. % % Information related to '81.253.182.0 - 81.253.185.255' % % Abuse contact for '81.253.182.0 - 81.253.185.255' is 'gestionip.ft@orange.com'  inetnum:      81.253.182.0 - 81.253.185.255 netname:      RBCI descr:        France Telecom Network country:      FR</pre>	<p>L'adresse IP appartient à RBCI, qui appartient au groupe orange, une FAI.</p>
---	--

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.

<pre> nic-hdl:      LLC359-FRNIC type:         ORGANIZATION contact:      Lycee Le Castel address:      Lycee Le Castel address:      4 boulevard Copernic address:      77420 Champs-sur-Marne </pre>	Le nom de domaine appartient au lycée Le Castel.
<pre> domain:      btsinfo.fr status:      ACTIVE eppstatus:   active hold:        NO holder-c:    LLC359-FRNIC admin-c:     LLC359-FRNIC tech-c:      G768-FRNIC registrar:   GANDI Expiry Date: 2025-06-08T14:50:06Z </pre>	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)

<a href="http://ping.eu/">http://ping.eu/</a>	<a href="http://www.subnetonline.com/pages/network-tools/online-tracepath.php">http://www.subnetonline.com/pages/network-tools/online-tracepath.php</a>
<pre> --- PING www.afrinic.net(2001:42d0:0:250::4) 56 data bytes --- 64 bytes from 2001:42d0:0:250::4: icmp_seq=1 ttl=57 time=170 ms 64 bytes from 2001:42d0:0:250::4: icmp_seq=2 ttl=57 time=170 ms 64 bytes from 2001:42d0:0:250::4: icmp_seq=3 ttl=57 time=169 ms 64 bytes from 2001:42d0:0:250::4: icmp_seq=4 ttl=57 time=170 ms  --- www.afrinic.net ping statistics ---      packets transmitted 4     received            4     packet loss          0 %     time                3008 ms  --- Round Trip Time (rtt) ---      min   169.478 ms     avg   169.576 ms     max   169.634 ms     mdev   0.059 ms </pre>	<pre> TracePath Output: 1?: [LOCALHOST]                                pmtu 1500 1: nova.subnetonline.com                       0.156ms reached 1: nova.subnetonline.com                       0.049ms reached Resume: pmtu 1500 hops 1 back 1  ---- Finished ----- </pre>

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 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 :

<pre>C:\Users\uti029&gt;pathping www.root-me.org Détermination de l'itinéraire vers www.root-me.org [212.129.28.16] avec un maximum de 30 sauts :  0 B181-102.sio.local [172.31.1.53]  1 172.31.1.254  2 100.100.1.160  3 46.18.224.51  4 * * * Traitement des statistiques pendant 75 secondes... Source vers ici  Ce nœud/Lien Saut RTT Perdu/Envoyé = % Perdu/Envoyé = % Adresse 0 0ms 0/ 100 = 0% 0/ 100 = 0% B181-102.sio.local [172.31.1.53] 1 0ms 0/ 100 = 0% 0/ 100 = 0% 172.31.1.254 2 0ms 0/ 100 = 0% 0/ 100 = 0% 100.100.1.160 3 0ms 0/ 100 = 0% 0/ 100 = 0% 46.18.224.51 Itinéraire déterminé.</pre>	<p>Il y a 3 sauts.</p>
--	------------------------

### 1.2.2 : Utilisation de la fonction nslookup :

<pre>C:\Users\uti029&gt;type %windir%\system32\drivers\etc\hosts. # Copyright (c) 1993-2009 Microsoft Corp. # # This is a sample HOSTS file used by Microsoft TCP/IP for Windows. # # This file contains the mappings of IP addresses to host names. Each # entry should be kept on an individual line. The IP address should # be placed in the first column followed by the corresponding host name. # The IP address and the host name should be separated by at least one # space. # # Additionally, comments (such as these) may be inserted on individual # lines or following the machine name denoted by a '#' symbol. # # For example: # #      102.54.94.97      rhino.acme.com      # source server #      38.25.63.10      x.acme.com         # x client host # # localhost name resolution is handled within DNS itself. # #      127.0.0.1        localhost #      ::1              localhost</pre>	<p>La commande type permet d'afficher le contenu d'un fichier, ici %windir%\system32\drivers\etc\hosts</p>
---	--

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.

<pre>C:\Windows\System32&gt;notepad C:\Windows\System32\drivers\etc\hosts</pre> <pre># Copyright (c) 1993-2009 Microsoft Corp. # # This is a sample HOSTS file used by Microsoft TCP/IP for Windows. # # This file contains the mappings of IP addresses to host names. Each # entry should be kept on an individual line. The IP address should # be placed in the first column followed by the corresponding host name. # The IP address and the host name should be separated by at least one # space. # # Additionally, comments (such as these) may be inserted on individual # lines or following the machine name denoted by a '#' symbol. # # For example: # # 102.54.94.97 rhino.acme.com      # source server # 38.25.63.10  x.acme.com        # x client host # # localhost name resolution is handled within DNS itself. # # 127.0.0.1 localhost # ::1 localhost 127.0.0.1 www.root-me.org 172.31.1.106 Shayma</pre>	<p>Ouvrir le fichier host</p> <p>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.</p>
<pre>C:\Windows\System32&gt;ping Shayma</pre> <pre>Envoi d'une requête 'ping' sur Shayma [172.31.1.106] avec 32 octets de données : Réponse de 172.31.1.106 : octets=32 temps=1 ms TTL=128 Réponse de 172.31.1.106 : octets=32 temps=1 ms TTL=128 Réponse de 172.31.1.106 : octets=32 temps&lt;1ms TTL=128 Réponse de 172.31.1.106 : octets=32 temps&lt;1ms TTL=128  Statistiques Ping pour 172.31.1.106:     Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),     Durée approximative des boucles en millisecondes :         Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms</pre>	<p>Ping vers Shayma.</p>

b)

<pre>/displaydns Affiche le contenu du cache de résolution DNS.</pre>	<p>On a plus qu'à chercher <a href="http://www.root-me.org">www.root-me.org</a> pour trouver son temps de conservation.</p>
<pre>www.root-me.org ----- Nom d'enregistrement. : www.root-me.org Type d'enregistrement : 1 Durée de vie . . . . : 7153 Longueur de données . : 4 Section . . . . . : Réponse Enregistrement (hôte) : 212.129.28.16</pre>	<p>Le temps de conservation est de 7153 secondes, 1 heure, 59 minutes et 13 secondes.</p>

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)

<pre> Entrer le nom de domaine a ajouter au fichier host :www.root-me.org Entrer l ip vers laquelle doit pointer le host (default: 127.0.0.1) :127.0.0.1 Nouvelle ligne inseree dans le fichier host </pre>	<p>Il permet d'ajouter un nom de domaine et l'adresse IP dans le fichier host.</p>
<pre> C:\Users\uti029&gt;type %windir%\system32\drivers\etc\hosts. # Copyright (c) 1993-2009 Microsoft Corp. # # This is a sample HOSTS file used by Microsoft TCP/IP for Windows. # # This file contains the mappings of IP addresses to host names. Each # entry should be kept on an individual line. The IP address should # be placed in the first column followed by the corresponding host name. # The IP address and the host name should be separated by at least one # space. # # Additionally, comments (such as these) may be inserted on individual # lines or following the machine name denoted by a '#' symbol. # # For example: # #       102.54.94.97       rhino.acme.com       # source server #       38.25.63.10      x.acme.com           # x client host # # localhost name resolution is handled within DNS itself. #       127.0.0.1         localhost #       ::1               localhost 127.0.0.1 www.root-me.org 127.0.0.1 www.root-me.org </pre>	<p>Il a bien été ajouté dans le fichier host.</p>

## 1.2.3 : Utilisation de nmap :

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

<pre> C:\Users\uti029&gt;nmap 172.31.64.1 Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-29 08:42 Paris, Madrid Nmap scan report for 172.31.64.1 Host is up (0.000026s latency). Not shown: 994 closed tcp ports (reset) PORT      STATE SERVICE 135/tcp   open  msrpc 139/tcp   open  netbios-ssn 445/tcp   open  microsoft-ds 2179/tcp  open  vmrpd 5432/tcp  open  postgresql 16992/tcp open  amt-soap-http Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds </pre>	<p>Les ports ouverts :</p> <p>135 : msrpc communique entre applications distribuées sur le réseau.</p> <p>139 : netbios-ssn partage des fichiers et des imprimantes sur des réseaux Windows.</p> <p>445 : microsoftds partage des fichiers, d'imprimantes et accéder aux ressources sur un réseau Windows.</p> <p>2179 : vmrpd contrôle à distance des machines virtuelles.</p> <p>5432 : PostgreSQL gère les connexions client-serveur d'SQL.</p> <p>16992 : amt-soap-http gère les ordinateurs même lorsqu'ils sont éteints ou hors du système d'exploitation.</p>
---	--

- 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.



```
C:\Users\uti029>nmap -f 172.31.64.1
Warning: Packet fragmentation selected on a host other than Linux, OpenBSD, FreeBSD, or NetBSD. This may or may not work.
Starting Nmap 7.95 ( https://nmap.org ) at 2024-12-02 09:24 Paris, Madrid
Stats: 0:00:31 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 15.00% done; ETC: 09:27 (0:02:01 remaining)
Stats: 0:00:33 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 16.00% done; ETC: 09:27 (0:02:59 remaining)
Stats: 0:00:34 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 16.50% done; ETC: 09:27 (0:02:57 remaining)
Stats: 0:00:35 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 17.00% done; ETC: 09:27 (0:02:56 remaining)
Stats: 0:00:37 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 18.00% done; ETC: 09:27 (0:02:52 remaining)
Stats: 0:00:38 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 18.50% done; ETC: 09:27 (0:02:52 remaining)
Stats: 0:00:39 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 19.00% done; ETC: 09:27 (0:02:51 remaining)
Stats: 0:00:40 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 19.50% done; ETC: 09:27 (0:02:49 remaining)
Stats: 0:00:45 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 22.00% done; ETC: 09:27 (0:02:43 remaining)
Stats: 0:00:46 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 22.50% done; ETC: 09:27 (0:02:42 remaining)
Stats: 0:00:47 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 23.00% done; ETC: 09:27 (0:02:41 remaining)
Stats: 0:00:48 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 23.50% done; ETC: 09:27 (0:02:40 remaining)
Stats: 0:00:49 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 24.00% done; ETC: 09:27 (0:02:38 remaining)
```

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 bloque pas mais les signale contrairement aux IPS qui les bloquent.

### 1.2.3.2 : Scanne des ports spécifiques :

```
C:\Users\uti029>nmap -p 22,80,443 172.31.64.1
Starting Nmap 7.95 ( https://nmap.org ) at 2024-12-02 09:35 Paris, Madrid
Nmap scan report for 172.31.64.1
Host is up (0.00s latency).

PORT      STATE SERVICE
22/tcp    closed ssh
80/tcp    closed http
443/tcp    closed https

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

- En limitant les scans à certains ports nous gagnons du temps et de la lisibilité en allant 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 intéressent 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 pare-feux. En limitant le nombre de ports scannés, il est possible de rester plus discret et d'éviter d'alerter les systèmes de sécurité.

```
C:\Users\uti029>nmap -p 22,80,443 172.31.64.1
Starting Nmap 7.95 ( https://nmap.org ) at 2024-12-02 09:35 Paris, Madrid
Nmap scan report for 172.31.64.1
Host is up (0.00s latency).

PORT      STATE SERVICE
22/tcp    closed ssh
80/tcp    closed http
443/tcp    closed https

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

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

### 1.2.3.3 Scanne de service et gestion :

<pre>C:\Users\uti029&gt;nmap -sV 172.31.64.1 Starting Nmap 7.95 ( https://nmap.org ) at 2024-12-02 09:37 Paris, Madrid Nmap scan report for 172.31.64.1 Host is up (0.000010s latency). Not shown: 994 closed tcp ports (reset) PORT      STATE SERVICE        VERSION 135/tcp    open  msrpc          Microsoft Windows RPC 139/tcp    open  netbios-ssn    Microsoft Windows netbios-ssn 445/tcp    open  microsoft-ds? 2179/tcp   open  vmrpd? 5432/tcp   open  postgresql     PostgreSQL DB 16992/tcp  open  http           Intel AMT WebUI 16.1.32.2418 (Standard Manageability) Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows  Service detection performed. Please report any incorrect results at https://nmap.org/submit/ Nmap done: 1 IP address (1 host up) scanned in 22.86 seconds</pre>	<p>135 : un service msrpc et avec une version Windows RPC.</p> <p>139 : un service netbios-ssn et avec une version Microsoft Windows netbios-ssn.</p> <p>445 : un service peut être microsoft-ds et avec une version inconnue</p> <p>2179 : un service peut être vmrpd et avec une version inconnue.</p> <p>5432 : un service postgresql et avec une version PostgreSQL DB.</p> <p>16992 : un service http et avec une version Intel AMT WebUI 16.1.32.2418 (Standard Manageability).</p>
---	---

- 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 pare-feux pour restreindre l'accès aux ports vulnérables et segmenter le réseau pour isoler les services obsolètes.

### 1.2.3.4 : Scanne avec détection d'OS :

<pre>C:\Users\uti029&gt;nmap -O 172.31.64.1 Starting Nmap 7.95 ( https://nmap.org ) at 2024-12-02 12:56 Paris, Madrid Nmap scan report for 172.31.64.1 Host is up (0.00027s latency). Not shown: 994 closed tcp ports (reset) PORT      STATE SERVICE        VERSION 135/tcp    open  msrpc          Microsoft Windows RPC 139/tcp    open  netbios-ssn    Microsoft Windows netbios-ssn 445/tcp    open  microsoft-ds? 2179/tcp   open  vmrpd? 5432/tcp   open  postgresql     PostgreSQL DB 16992/tcp  open  amt-soap-http Device type: general purpose Running: Microsoft Windows 10 11 OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_11 OS details: Microsoft Windows 10 1607 - 11 23H2 Network Distance: 0 hops  OS detection performed. Please report any incorrect results at https://nmap.org/submit/ Nmap done: 1 IP address (1 host up) scanned in 1.23 seconds</pre>	<p>C'est moyennement fiable car il me propose deux OS : Microsoft Windows 10 et Microsoft Windows 11.</p>
--	---

- 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 :

<pre>C:\Users\uti029&gt;nmap -sS 172.31.64.1 Starting Nmap 7.95 ( https://nmap.org ) at 2024-12-02 13:09 Paris, Madrid Nmap scan report for 172.31.64.1 Host is up (0.000023s latency). Not shown: 994 closed tcp ports (reset) PORT      STATE SERVICE 135/tcp   open  msrpc 139/tcp   open  netbios-ssn 445/tcp   open  microsoft-ds 2179/tcp  open  vmrpd 5432/tcp  open  postgresql 16992/tcp open  amt-soap-http  Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds</pre>	<p>Il y a juste le temps de latence qui est 3 fois moins élevée sur un scan furtif par rapport à un scan standard.</p>
<pre>C:\Users\uti029&gt;nmap 172.31.64.1 Starting Nmap 7.95 ( https://nmap.org ) at 2024-12-02 13:09 Paris, Madrid Nmap scan report for 172.31.64.1 Host is up (0.0000070s latency). Not shown: 994 closed tcp ports (reset) PORT      STATE SERVICE 135/tcp   open  msrpc 139/tcp   open  netbios-ssn 445/tcp   open  microsoft-ds 2179/tcp  open  vmrpd 5432/tcp  open  postgresql 16992/tcp open  amt-soap-http  Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds</pre>	

- 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 :

<pre> C:\Users\uti029&gt;nmap --script vuln 172.31.64.1 Starting Nmap 7.95 ( https://nmap.org ) at 2024-12-02 13:12 Paris, Madrid Pre-scan script results:   broadcast-avahi-dos:     Discovered hosts:       224.0.0.251       After NULL UDP avahi packet DoS (CVE-2011-1002).       Hosts are all up (not vulnerable). Nmap scan report for 172.31.64.1 Host is up (0.80075s latency). Not shown: 994 closed tcp ports (reset) PORT      STATE SERVICE 1138/tcp  open  mape 139/tcp   open  netbios-ssn 445/tcp   open  microsoft-ds 2179/tcp  open  vmrpd 5432/tcp  open  postgresql 16992/tcp open  ant-soap-http  Host script results:  _samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR  _smb-vuln-ms10-054: false  _smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR Nmap done: 1 IP address (1 host up) scanned in 66.14 seconds </pre>	<p>Il n'y a pas de vulnérabilité détectée.</p>
--	--

- 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.

```
C:\Users\uti029>nmap -sV 172.31.1.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2024-12-06 14:21 Paris, Madrid
^C
C:\Users\uti029>nmap -sL 172.31.1.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2024-12-06 14:21 Paris, Madrid
Nmap scan report for 172.31.1.0
Nmap scan report for al-esxi-01.sio.local (172.31.1.1)
Nmap scan report for al-esxi-02.sio.local (172.31.1.2)
Nmap scan report for al-esxi-03.sio.local (172.31.1.3)
Nmap scan report for AL-DC-01.sio.local (172.31.1.4)
Nmap scan report for 172.31.1.5
Nmap scan report for AL-DC-02.sio.local (172.31.1.6)
Nmap scan report for AL-VEEAM.sio.local (172.31.1.7)
Nmap scan report for AL-WSUS.sio.local (172.31.1.8)
Nmap scan report for SRV-SIO-GHOST2.sio.local (172.31.1.9)
Nmap scan report for al-vcsa.sio.local (172.31.1.10)
Nmap scan report for al-esxi-01-idrac.sio.local (172.31.1.11)
Nmap scan report for al-esxi-02-idrac.sio.local (172.31.1.12)
Nmap scan report for al-esxi-03-idrac.sio.local (172.31.1.13)
Nmap scan report for 172.31.1.14
Nmap scan report for SRV-MSTREAM.sio.local (172.31.1.15)
Nmap scan report for 172.31.1.16
Nmap scan report for 172.31.1.17
Nmap scan report for 172.31.1.18
Nmap scan report for 172.31.1.19
Nmap scan report for 172.31.1.20
Nmap scan report for 172.31.1.21
```

On commence par scanner pour voir tous les appareils du réseau (-sL).

```
C:\Users\uti029>nmap -sn 172.31.1.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2024-12-06 14:22 Paris, Madrid
Nmap scan report for al-esxi-01.sio.local (172.31.1.1)
Host is up (0.0010s latency).
MAC Address: E4:43:4B:71:EA:E4 (Dell)
Nmap scan report for al-esxi-02.sio.local (172.31.1.2)
Host is up (0.0010s latency).
MAC Address: E4:43:4B:71:E8:00 (Dell)
Nmap scan report for al-esxi-03.sio.local (172.31.1.3)
Host is up (0.0010s latency).
MAC Address: E4:43:4B:71:E9:74 (Dell)
Nmap scan report for AL-DC-01.sio.local (172.31.1.4)
Host is up (0.00s latency).
MAC Address: 00:19:99:B7:BF:26 (Fujitsu Technology Solutions GmbH)
Nmap scan report for AL-DC-02.sio.local (172.31.1.6)
Host is up (0.00s latency).
MAC Address: 00:50:56:B7:C9:34 (VMware)
Nmap scan report for AL-VEEAM.sio.local (172.31.1.7)
Host is up (0.00s latency).
MAC Address: 00:50:56:B7:54:A5 (VMware)
Nmap scan report for AL-WSUS.sio.local (172.31.1.8)
Host is up (0.00s latency).
MAC Address: 00:50:56:B7:A8:EB (VMware)
Nmap scan report for al-vcsa.sio.local (172.31.1.10)
Host is up (0.00s latency).
MAC Address: 00:0C:29:97:F2:EC (VMware)
Nmap scan report for al-esxi-01-idrac.sio.local (172.31.1.11)
Host is up (0.0010s latency).
```

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 :

```
C:\Users\uti029>nmap -sV 172.31.1.4
Starting Nmap 7.95 ( https://nmap.org ) at 2024-12-06 14:23 Paris, Madrid
Nmap scan report for AL-DC-01.sio.local (172.31.1.4)
Host is up (0.00055s latency).
Not shown: 986 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
53/tcp    open  domain         Simple DNS Plus
88/tcp    open  kerberos-sec   Microsoft Windows Kerberos (server time: 2024-12-06 13:23:05Z)
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
389/tcp   open  ldap           Microsoft Windows Active Directory LDAP (Domain: sio.local, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds   Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: SIO)
464/tcp   open  kpasswd5?      Microsoft Windows RPC over HTTP 1.0
593/tcp   open  ncacn_http     Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap           Microsoft Windows Active Directory LDAP (Domain: sio.local, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server  Microsoft Terminal Services
5985/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
7070/tcp  open  ssl/realserver?
MAC Address: 00:19:99:B7:BF:26 (Fujitsu Technology Solutions GmbH)
Service Info: Host: AL-DC-01; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.85 seconds
```

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

```
C:\Users\uti029>nmap -sV 172.31.1.8
Starting Nmap 7.95 ( https://nmap.org ) at 2024-12-06 14:28 Paris, Madrid
Nmap scan report for AL-WSUS.sio.local (172.31.1.8)
Host is up (0.0011s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE        VERSION
80/tcp    open  http           Microsoft IIS httpd 10.0
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds   Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp  open  ms-wbt-server  Microsoft Terminal Services
5985/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
7070/tcp  open  ssl/realserver?
MAC Address: 00:50:56:B7:A8:EB (VMware)
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.77 seconds
C:\Users\uti029>
```

Celle-ci a été choisie délibérément server wsus indique que c'est un serveur 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 crée

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 métaexploit :

Sous linux Ubuntu :

<pre>root@B181-102:~# sudo apt update sudo apt upgrade -y Get:1 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB] Hit:2 http://archive.ubuntu.com/ubuntu noble InRelease Get:3 http://archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB] Get:4 http://archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB] Get:5 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [498 kB] Get:6 http://archive.ubuntu.com/ubuntu noble/universe amd64 Packages [15.0 MB] Get:7 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [102 kB] Get:8 http://security.ubuntu.com/ubuntu noble-security/main amd64 Components [7188 B] Get:9 http://security.ubuntu.com/ubuntu noble-security/main amd64 c-n-f Metadata [5892 B] Get:10 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [563 kB] Get:11 http://security.ubuntu.com/ubuntu noble-security/universe Translation-en [150 kB] Get:12 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [51.9 kB] Get:13 http://security.ubuntu.com/ubuntu noble-security/universe amd64 c-n-f Metadata [13. Get:14 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Packages [480 kB] Get:15 http://security.ubuntu.com/ubuntu noble-security/restricted Translation-en [92.5 kB] Get:16 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Components [212 B]</pre>	<pre>sudo apt update sudo apt upgrade -y</pre>
---	--

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

```
root@B181-102:~# git clone https://github.com/offensive-security/exploitdb.git /opt/exploitdb
Cloning into '/opt/exploitdb'...
remote: Enumerating objects: 215620, done.
remote: Counting objects: 100% (5/5), done.
remote: Compressing objects: 100% (4/4), done.
Receiving objects: 0% (1181/215620), 588.01 KiB | 203.00 KiB/s
```

```
root@B181-102:~# snap install searchsploit
Download snap "snapd" (23258) from channel "stable"
```

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

Maintenant que l'on a analysé que l'active directory avait une version service http liée au service RCP :

```
root@B181-102:~# searchsploit RCP 1.0
```

Exploit Title	Path
Dan Bernstein QMail 1.0 3 - RCPT Denial of Service (1)	linux/dos/20561.pl
Dan Bernstein QMail 1.0 3 - RCPT Denial of Service (2)	linux/dos/20562.c
MyBB 1.0.1/1.0.2 Notepad - 'user_rcp.php' HTML Injection	php/webapps/27122.txt
MyBulletinBoard (MyBB) 1.0 - 'user_rcp.php' SQL Injection	php/webapps/26396.pl
MyBulletinBoard (MyBB) 1.0.x/1.1.x - 'user_rcp.php' SQL Injection	php/webapps/28092.txt

```
Shellcodes: No Results
root@B181-102:~#
```

Chaque liste que vous voyez ici est une faille de sécurité publique et connue répertoriée sur exploit db, il serait important d'effectuer les mises à jour car ce sont de simples failles de sécurité que l'on peut corriger facilement.



## 1.2.3.7.4 : Analyse Wsus :

```

C:\Users\uti029>nmap -sV 172.31.1.8
Starting Nmap 7.95 ( https://nmap.org ) at 2024-12-06 14:28 Paris, Madrid
Nmap scan report for AL-W\SUS.sio.local (172.31.1.8)
Host is up (0.0014s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE          VERSION
80/tcp    open  http             Microsoft IIS httpd 10.0
135/tcp    open  msrpc            Microsoft Windows RPC
139/tcp    open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds    Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp   open  ms-wbt-server    Microsoft Terminal Services
5985/tcp   open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
7070/tcp   open  ssl/realserver?
MAC Address: 00:50:56:B7:A8:EB (VMware)
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.77 seconds

```

root@B181-102:~# searchsploit httpd 2.0		On voit toutes les failles de l'httd 2.0 en rouge
Exploit Title	Path	
Acme httd 1.9/2.0.x - CGI Test Script Cross-Site Scripting	cgi/remote/23582.txt	
Acme httd 2.0.7 - Directory Traversal	windows/remote/24350.txt	
Apache - Arbitrary Long HTTP Headers (Denial of Service)	multiple/dos/360.pl	
Apache - Arbitrary Long HTTP Headers Denial of Service	linux/dos/371.c	
Apache 1.1 / NCSA HTtd 1.5.2 / Netscape Server 1.12/1.1/2.0 - a nph-test	multiple/dos/19536.txt	
Apache 1.3.x < 2.0.48 mod_userdir - Remote Users Disclosure	linux/remote/132.c	
Apache 2.0.44 (Linux) - Remote Denial of Service	linux/dos/11.c	
Apache 2.0.45 - 'APR' Crash	linux/dos/38.pl	
Apache 2.0.49 - Arbitrary Long HTTP Headers Denial of Service	multiple/dos/1856.pl	
Apache 2.0.52 - GET Denial of Service	multiple/dos/855.pl	
Apache 2.x - Memory Leak	windows/dos/9.c	
D-Link DML-G700AP 2.00/2.01 - HTtd Denial of Service	hardware/dos/27241.c	
Omnicron OmniHTtd 1.1/2.0 Alpha 1 - 'visiadmin.exe' Denial of Service	windows/dos/20304.txt	
Omnicron OmniHTtd 2.0.4-8 - File Source Disclosure	windows/remote/20886.txt	
Omnicron OmniHTtd 2.0.7 - File Corruption / Command Execution	windows/remote/20557.pl	
OmniHTtd 1.1/2.0.x/2.4 - 'test.php' Sample Application Cross-Site Script	windows/remote/21753.txt	
OmniHTtd 1.1/2.0.x/2.4 - Sample Application URL Encoded Newline HTML Inj	windows/remote/21757.txt	
OmniHTtd 1.1/2.0.x/2.4 - test.shtml Sample Application Cross-Site Script	windows/remote/21754.txt	
OpenBSD HTtd < 6.0 - Memory Exhaustion Denial of Service	openbsd/dos/41278.txt	
RaidenHTtd 2.0.19 - 'ulang' Remote Command Execution	windows/remote/4747.vbs	
Shellcodes: No Results		
root@B181-102:~#		

root@B181-102:~# searchsploit httpd 10	
Exploit Title	Path
ACME micro_httd - Denial of Service	linux/dos/34102.py
Acme httd 1.9/2.0.x - CGI Test Script Cross-Site Scripting	cgi/remote/23582.txt
Acme httd 2.0.7 - Directory Traversal	windows/remote/24350.txt
Acme httd HTTP Server - Directory Traversal	linux/remote/38522.txt
AN HTtd - 'CMDIS.dll' Remote Buffer Overflow (PoC)	windows/dos/25364.txt
AN HTtd 1.38/1.39/1.40/1.41 - 'SOCKS4' Buffer Overflow	windows/remote/21955.java
AN HTtd 1.41 e - Cross-Site Scripting	multiple/remote/22130.txt
AN HTtd 1.42 - Arbitrary Log Content Injection	windows/remote/25365.txt
Apache 1.1 / NCSA HTtd 1.5.2 / Netscape Server 1.12/1.1/2.0 - a nph-test	multiple/dos/19536.txt
Apache 2.0.44 (Linux) - Remote Denial of Service	linux/dos/11.c
Apache 2.0.49 - Arbitrary Long HTTP Headers Denial of Service	multiple/dos/1856.pl
Apache 2.x - Memory Leak	windows/dos/9.c
Apache HTTP Server 2.4.49 - Path Traversal & Remote Code Execution (RCE)	multiple/webapps/50383.sh
Apache HTtd mod_proxy - Error Page Cross-Site Scripting	multiple/webapps/47688.md
Apache HTtd mod_rewrite - Open Redirects	multiple/webapps/47689.md
Apache Tomcat mod_jk 1.2.20 - Remote Buffer Overflow (Metasploit)	windows/remote/16798.rb
ATP HTtd 0.4 - Single Byte Buffer Overflow	linux/remote/21936.c
CoreHTTP 0.5.3alpha - HTtd Remote Buffer Overflow	linux/remote/4243.c
DD-WRT HTtd Daemon/Service - Arbitrary Command Execution (Metasploit)	cgi/webapps/16856.rb
DD-WRT HTtd Daemon/Service - Remote Command Execution	hardware/remote/9209.txt
DomsHTtd 1.0 - Remote Denial of Service	windows/dos/19866.pl
gnttd 1.4.x - 'Log()' Remote Buffer Overflow	linux/remote/21937.c
httdasm 0.92 - Directory Traversal	windows/remote/15861.txt
httdasm 0.92 - Remote Buffer Overflow (Metasploit)	windows/remote/16680.txt



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

Structure du Fichier analyse.bat :

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

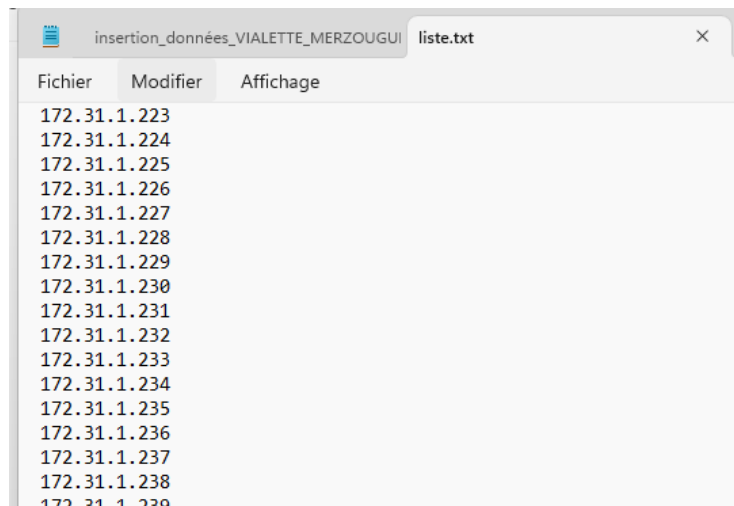
```
Fichier  Modifier  Affichage

nmap -iL liste.txt -sV >> log-nmap-.txt
```

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 :



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:\Users\uti029>route print -4

=====
Liste d'Interfaces
18...00 15 5d b9 10 53 .....Hyper-V Virtual Ethernet Adapter
17...e0 73 e7 b2 64 d7 .....Intel(R) Ethernet Connection (17) I219-LM
9...0a 09 27 00 00 09 .....VirtualBox Host-Only Ethernet Adapter
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    172.31.1.53     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         172.31.1.53     281
172.31.1.53        255.255.255.255 On-Link         172.31.1.53     281
172.31.1.255       255.255.255.255 On-Link         172.31.1.53     281
172.31.64.0        255.255.240.0  On-Link         172.31.64.1     271
172.31.64.1        255.255.255.255 On-Link         172.31.64.1     271
172.31.79.255      255.255.255.255 On-Link         172.31.64.1     271
192.168.56.0       255.255.255.0  On-Link         192.168.56.1    281
192.168.56.1       255.255.255.255 On-Link         192.168.56.1    281
192.168.56.255     255.255.255.255 On-Link         192.168.56.1    281
224.0.0.0          240.0.0.0      On-Link         127.0.0.1       331
224.0.0.0          240.0.0.0      On-Link         192.168.56.1    281
224.0.0.0          240.0.0.0      On-Link         172.31.1.53     281
224.0.0.0          240.0.0.0      On-Link         172.31.64.1     271
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         192.168.56.1    281
255.255.255.255    255.255.255.255 On-Link         172.31.1.53     281
255.255.255.255    255.255.255.255 On-Link         172.31.64.1     271
=====
Itinéraires persistants :
Aucun

```

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.

```

C:\Users\uti029>route print -6
=====
Liste d'Interfaces
18...00 15 5d b9 10 53 .....Hyper-V Virtual Ethernet Adapter
17...e0 73 e7 b2 64 d7 .....Intel(R) Ethernet Connection (17) I219-LM
9...0a 00 27 00 00 09 .....VirtualBox Host-Only Ethernet Adapter
1.....Software Loopback Interface 1
45...00 15 5d 49 46 21 .....Hyper-V Virtual Ethernet Adapter #2
=====

IPv6 Table de routage
=====
Itinéraires actifs :
If Metric Network Destination Gateway
1 331 ::1/128 On-link
9 281 fe80::764 On-link
17 281 fe80::/64 On-link
18 271 fe80::/64 On-link
45 5256 fe80::/64 On-link
45 5256 fe80::10a0:82fc:9fa2:9a63/128 On-link
9 281 fe80::6b0e:fbaf:d48e:8bd1/128 On-link
17 281 fe80::dd7c:ed8b:e875:d983/128 On-link
18 271 fe80::e343:3979:f75b:d1a9/128 On-link
1 331 ff00::/8 On-link
9 281 ff00::/8 On-link
17 281 ff00::/8 On-link
18 271 ff00::/8 On-link
45 5256 ff00::/8 On-link
=====
Itinéraires persistants :
Aucun

```

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)

```

C:\Users\uti029>netsh
netsh>interface
netsh interface>ipv4
netsh interface ipv4>show interfaces

```

Idx	Mét	MTU	État	Nom
1	75	4294967295	connected	Loopback Pseudo-Interface 1
17	25	1500	connected	Ethernet
9	25	1500	connected	Ethernet 2
18	15	1500	connected	vEthernet (Default Switch)

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)

```

C:\Users\uti029>netsh
netsh>interface
netsh interface>show interface

```

État admin	État	Type	Nom de l'interface
Activé	Connecté	Dédié	Ethernet 2
Activé	Connecté	Dédié	Ethernet

```

netsh interface>

```

- 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.

<pre> netsh interface&gt;ipv6 netsh interface ipv6&gt;show neighbors  Interface 1 : Loopback Pseudo-Interface 1  Adresse Internet          Adresse physique  Type ----- ff02::16                  33-33-00-00-00-02 Permanent ff02::1:2                  33-33-00-00-00-16 Permanent  Interface 17 : Ethernet  Adresse Internet          Adresse physique  Type ----- ff02::1                    33-33-00-00-00-01 Permanent ff02::2                    33-33-00-00-00-02 Permanent ff02::16                   33-33-00-00-00-16 Permanent ff02::fb                   33-33-00-00-00-fb Permanent ff02::1:2                  33-33-00-01-00-02 Permanent ff02::1:3                  33-33-00-01-00-03 Permanent ff02::1:ff75:d983          33-33-ff-75-d9-83 Permanent  Interface 9 : Ethernet 2  Adresse Internet          Adresse physique  Type ----- ff02::1                    33-33-00-00-00-01 Permanent ff02::2                    33-33-00-00-00-02 Permanent ff02::16                   33-33-00-00-00-16 Permanent ff02::fb                   33-33-00-00-00-fb Permanent ff02::1:2                  33-33-00-01-00-02 Permanent ff02::1:3                  33-33-00-01-00-03 Permanent ff02::1:ff8e:8bd1          33-33-ff-8e-8b-d1 Permanent  Interface 18 : vEthernet (Default Switch)  Adresse Internet          Adresse physique  Type ----- ff02::1                    33-33-00-00-00-01 Permanent ff02::2                    33-33-00-00-00-02 Permanent ff02::16                   33-33-00-00-00-16 Permanent ff02::fb                   33-33-00-00-00-fb Permanent ff02::1:2                  33-33-00-01-00-02 Permanent ff02::1:3                  33-33-00-01-00-03 Permanent ff02::1:ff5b:d1a9          33-33-ff-5b-d1-a9 Permanent </pre>	<p>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.</p>
--	---

c)

<pre> C:\Users\uti029&gt;Netsh netsh&gt;int netsh interface&gt;ip reset Réinitialisation de Transfert de compartiment réussie. Réinitialisation de Compartiment réussie. Réinitialisation de Protocole de contrôle réussie. Réinitialisation de Requête de séquence d'échos réussie. Échec de la réinitialisation de Général. L'opération demandée requiert une élévation (Exécuter en tant qu'administrateur). Échec de la réinitialisation de Interface. L'opération demandée requiert une élévation (Exécuter en tant qu'administrateur). Réinitialisation de Adresse anycast réussie. Réinitialisation de Adresse de multidiffusion réussie. Échec de la réinitialisation de Adresse unicast. L'opération demandée requiert une élévation (Exécuter en tant qu'administrateur). Échec de la réinitialisation de Voisin. L'opération demandée requiert une élévation (Exécuter en tant qu'administrateur). Échec de la réinitialisation de Chemin d'accès. L'opération demandée requiert une élévation (Exécuter en tant qu'administrateur). Réinitialisation de Potentiel réussie. Réinitialisation de Préfixe de stratégie réussie. Réinitialisation de Proxy voisin réussie. Réinitialisation de Routage réussie. Réinitialisation de Préfixe de site réussie. Réinitialisation de Sous-interface réussie. Réinitialisation de Motif d'éveil réussie. Réinitialisation de Résoudre le voisin réussie. Réinitialisation de réussie. Réinitialisation de réussie. Réinitialisation de réussie. Échec de la réinitialisation de . L'opération demandée requiert une élévation (Exécuter en tant qu'administrateur). Réinitialisation de réussie. Réinitialisation de réussie. Réinitialisation de réussie. Échec de la réinitialisation de . L'opération demandée requiert une élévation (Exécuter en tant qu'administrateur). Réinitialisation de réussie. Réinitialisation de réussie. Réinitialisation de réussie. Redémarrez l'ordinateur pour terminer cette action. </pre>	<p>Int ip pour indiquer que l'on souhaite travailler sur la pile IP.</p> <p>Rest pour réinitialiser aux valeurs par default.</p>
---	--

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.

```
netsh interface=netsh
netsh interface=ipnetsh
netsh interface=ipnetsh
netsh interface=ipnetsh

# Configuration du protocole IPv4
#
pushd interface ipv4

reset

set global
set interface interface="Ethernet (débogueur du noyau)" forwarding=enabled advertise=enabled nud=enabled ignoredefaultroutes=disabled
set interface interface="Ethernet" forwarding=enabled advertise=enabled nud=enabled ignoredefaultroutes=disabled
set interface interface="Ethernet 2" forwarding=enabled advertise=enabled nud=enabled ignoredefaultroutes=disabled
set interface interface="vEthernet (Default Switch)" forwarding=enabled advertise=enabled nud=enabled ignoredefaultroutes=disabled
add address name="Ethernet 2" address=192.168.56.1 mask=255.255.255.0
add address name="vEthernet (Default Switch)" address=172.31.64.1 mask=255.255.255.0

popd

# Fin de la configuration du protocole IPv4

netsh interface ipnetsh > sauvegarde_config_VialetteCandice.txt

# Configuration du protocole IPv4
#
pushd interface ipv4

reset

set global
set interface interface="Ethernet (débogueur du noyau)" forwarding=enabled advertise=enabled nud=enabled ignoredefaultroutes=disabled
set interface interface="Ethernet" forwarding=enabled advertise=enabled nud=enabled ignoredefaultroutes=disabled
set interface interface="Ethernet 2" forwarding=enabled advertise=enabled nud=enabled ignoredefaultroutes=disabled
set interface interface="vEthernet (Default Switch)" forwarding=enabled advertise=enabled nud=enabled ignoredefaultroutes=disabled
add address name="Ethernet 2" address=192.168.56.1 mask=255.255.255.0
add address name="vEthernet (Default Switch)" address=172.31.64.1 mask=255.255.255.0

popd

# Fin de la configuration du protocole IPv4
```

### 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).

```
C:\Windows\System32>netsh
netsh>advfirewall
netsh advfirewall>firewall
netsh advfirewall firewall>add rule name="Autoriser Chrome" dir=in action=allow program="C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" enable=yes
Ok.

netsh advfirewall firewall>add rule name="Blocage FTP" protocol=TCP dir=in localport=21 action=block
Ok.

netsh advfirewall firewall>show rule name="Autoriser Chrome"

Nom de la règle : Autoriser Chrome
-----
Activé : Oui
Direction : Actif
Profiles : Domaine,Privé,Public
Groupement :
LocalIP : Tout
RemoteIP : Tout
Protocole : Tout
Traversée latérale : Non
Action : Autoriser
Ok.
```

Nom de la règle :	Blocage FTP
Activé :	Oui
Direction :	Actif
Profils :	Domaine, Privé, Public
Groupe :	
LocalIP :	Tout
RemoteIP :	Tout
Protocole :	TCP
LocalPort :	21
RemotePort :	Tout
Traversée latérale :	Non
Action :	Bloquer
Ok.	

Les règles sont bien appliquées.

- Un pare-feu restreint ou permet d'accéder à des applications en fonction des règles 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 reconnaître 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 d'un scan de ports par des hackers. Il suit la connexion au réseau séparant le trafic légitime du trafic non sollicité.

```
netsh advfirewall firewall>delete rule name="Blocage FTP"
2 règle(s) supprimée(s).
Ok.
```

### 1.2.6 : Utilisation de la fonction netstat :

a)

C:\Users\uti029>netstat

Connexions actives

Proto	Adresse locale	Adresse distante	État
TCP	127.0.0.1:49671	www:49672	ESTABLISHED
TCP	127.0.0.1:49672	www:49671	ESTABLISHED
TCP	127.0.0.1:49703	www:49704	ESTABLISHED
TCP	127.0.0.1:49704	www:49703	ESTABLISHED
TCP	172.31.1.67:10036	AL-DC-01:49671	ESTABLISHED
TCP	172.31.1.67:10504	20.190.190.101:https	ESTABLISHED
TCP	172.31.1.67:11725	20.199.120.182:https	ESTABLISHED
TCP	172.31.1.67:11728	20.199.120.182:https	ESTABLISHED
TCP	172.31.1.67:11900	20.238.236.234:https	ESTABLISHED
TCP	172.31.1.67:11921	SRV-SIO:microsoft-ds	ESTABLISHED
TCP	172.31.1.67:11938	52.111.231.21:https	ESTABLISHED
TCP	172.31.1.67:12218	52.97.233.114:https	ESTABLISHED
TCP	172.31.1.67:12241	104.18.32.47:https	ESTABLISHED
TCP	172.31.1.67:12242	104.18.32.47:https	ESTABLISHED
TCP	172.31.1.67:12264	52.111.231.21:https	ESTABLISHED
TCP	172.31.1.67:12276	204.79.197.239:https	ESTABLISHED
TCP	172.31.1.67:12279	20.50.73.11:https	ESTABLISHED
TCP	172.31.1.67:12281	ec2-3-233-158-25:https	ESTABLISHED

Il y a que les ports TCP activés.

b)

```
C:\Users\uti029>netstat -e
Statistiques de l'interface
```

	Reçus	Émis
Octets	178368720	51521562
Paquets monodiffusion	182220	130350
Paquets non monodiffusion	147810	73884
Rejets	0	0
Erreurs	0	0
Protocoles inconnus	0	

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

c)

C:\Users\uti029>netstat -s

Statistiques IPv4

Paquets Reçus	=	788643
Erreurs d'en-tête reçues	=	0
Erreurs d'adresse reçues	=	338
Datagrammes transférés	=	0
Protocoles inconnus reçus	=	4
Paquets reçus rejetés	=	8237
Paquets reçus délivrés	=	822942
Requêtes en sortie	=	609366
Routages rejetés	=	0
Paquets en sortie rejetés	=	1491
Paquet en sortie non routés	=	286
Réassemblage requis	=	6
Réassemblage réussi	=	3
Défaillances de réassemblage	=	0
Fragmentations de datagrammes réussies	=	0
Fragmentations de datagrammes défaillantes	=	0
Fragments Créés	=	0

Statistiques ICMPv6

	Reçus	Émis
Messages	124	901
Erreurs	0	0
Destination inaccessible	0	0
Paquet trop grand	0	0
Temps dépassé	0	0
Problèmes de paramètres	0	0
Echos	0	0
Réponses échos	0	0
Requêtes MLD	0	0
Rapports MLD	0	0
MLD appliqués	0	0
Sollicitations des routeurs	0	485
Annonces des routeurs	0	0
Sollicitations du voisin	1	209
Annonces du voisin	123	207
Redirections	0	0
Renumerotation du routeur	0	0

Statistiques TCP pour IPv4

Ouvertures actives	=	13660
Ouvertures passives	=	606
Tentatives de connexion non réussies	=	2031
Connexions réinitialisées	=	2487
Connexions en cours	=	15
Segments reçus	=	520003
Segments envoyés	=	475758
Segments retransmis	=	2859

Le protocole le plus utilisé est l'IPv4

Statistiques IPv6

Paquets Reçus	=	89875
Erreurs d'en-tête reçues	=	0
Erreurs d'adresse reçues	=	0
Datagrammes transférés	=	0
Protocoles inconnus reçus	=	0
Paquets reçus rejetés	=	1493
Paquets reçus délivrés	=	106697
Requêtes en sortie	=	38735
Routages rejetés	=	0
Paquets en sortie rejetés	=	0
Paquet en sortie non routés	=	0
Réassemblage requis	=	0
Réassemblage réussi	=	0
Défaillances de réassemblage	=	0
Fragmentations de datagrammes réussies	=	0
Fragmentations de datagrammes défaillantes	=	0
Fragments Créés	=	0

Statistiques ICMPv4

	Reçus	Émis
Messages	1572	1048
Erreurs	0	0
Destination inaccessible	1222	678
Temps dépassé	32	0
Problèmes de paramètres	0	0
La source s'éteint	0	0
Redirections	0	0
Réponses échos	316	2
Echos	2	368
Dates	0	0
Réponses du dateur	0	0
Masques d'adresses	0	0
Réponses du masque d'adresses	0	0
Sollicitations des routeurs	0	0
Annonces des routeurs	0	0

Statistiques UDP pour IPv4			
Datagrammes reçus	= 342850		
Aucun port	= 6371		
Erreurs reçues	= 0		
Datagrammes envoyés	= 106752		
Statistiques UDP pour IPv6			
Datagrammes reçus	= 147996		
Aucun port	= 1235		
Erreurs reçues	= 0		
Datagrammes envoyés	= 19528		

d)

C:\Users\uti029>netstat -abno		netstat -abno
Connexions actives		
Proto	Adresse locale	Adresse distante
TCP	0.0.0.0:135	0.0.0.0:0
RpcSs		LISTENING
[svchost.exe]		1256
TCP	0.0.0.0:445	0.0.0.0:0
Impossible d'obtenir les informations de propriétaire		LISTENING
TCP	0.0.0.0:623	0.0.0.0:0
[LMS.exe]		4
TCP	0.0.0.0:2179	0.0.0.0:0
[vmms.exe]		LISTENING
TCP	0.0.0.0:5040	0.0.0.0:0
CDPSvc		2676
[svchost.exe]		LISTENING
TCP	0.0.0.0:5432	0.0.0.0:0
[postgres.exe]		7084
TCP	0.0.0.0:7680	0.0.0.0:0
Impossible d'obtenir les informations de propriétaire		LISTENING
TCP	0.0.0.0:16992	0.0.0.0:0
[LMS.exe]		10588
TCP	0.0.0.0:49664	0.0.0.0:0
[lsass.exe]		LISTENING
TCP	0.0.0.0:49665	0.0.0.0:0
Impossible d'obtenir les informations de propriétaire		LISTENING
TCP	0.0.0.0:49666	0.0.0.0:0
Schedule		5344
[svchost.exe]		1028
		984
		2492

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:\Users\uti029>Net share			
Nom partage	Ressource	Remarque	
C\$	C:\	Partage par défaut	C\$ est un partage administratif de la partition C:\, pour avoir accès à la racine du disque à distance. D\$ est similaire à C\$ mais 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.
D\$	D:\	Partage par défaut	
IPC\$		IPC distant	
print\$	C:\windows\system32\spool\drivers	Pilotes d'imprimantes	
ADMIN\$	C:\windows	Administration à distance	
La commande s'est terminée correctement.			

b)

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

C:\Users\uti029>Net computer \\SRV-SIO La syntaxe de cette commande est :  NET COMPUTER \\nom_ordinateur {/ADD   /DEL}		
PS C:\Users\uti029> net view B181-102 La liste est vide.  PS C:\Users\uti029> net view \\SRV-SIO Ressources partagées de \\SRV-SIO  Nom du partage    Type    Utilisé comme    Commentaire ----- Ressources        Disque    R: RessourcesProfs    Disque ressourcesws        Disque WinDesign          Disque La commande s'est terminée correctement. PS C:\Users\uti029>		Afficher les ressources partagées d'un ordinateur ou d'un serveur spécifique.
PS C:\Users\uti029> net view B181-102 /DOMAIN:\\SRV-SIO La liste est vide.		Il n'y a pas de ressources partagées dans mon ordinateur.

c)

<pre>PS C:\Users\uti029&gt; Net config workstation.Net config workstation La syntaxe de cette commande est :</pre>	
<pre>PS C:\Users\uti029&gt; net config workstation Nom de l'ordinateur                \\B181-102 Nom complet de l'ordinateur       B181-102.sio.local Nom d'utilisateur                  UTI029  Station active sur     NetBT_Tcpip_{31C2C39D-0079-4D6A-93B4-276C7DC99656} (00155DB91053)  Version du logiciel                Windows 10 Pro Education  Domaine de station                 SIO Nom DNS du domaine de la station de travail sio.local Domaine de connexion              SIO  Délai d'ouverture COM (s)         0 Compteur d'émission COM (octets)  16 Délai d'émission COM (ms)        250 La commande s'est terminée correctement.  PS C:\Users\uti029&gt; S </pre>	<p>Pour afficher des informations sur la configuration du poste.</p>

Net session	<pre>C:\Users\uti029&gt;Net session L'erreur système 5 s'est produite.  Accès refusé.</pre>	
Net session \\nom_ordinateur	<pre>C:\Users\uti029&gt;Net session \\B181-102 L'erreur système 5 s'est produite.  Accès refusé.</pre>	
Net start service	<pre>C:\Users\uti029&gt;Net start service Le nom de service n'est pas valide.  Vous obtiendrez une aide supplémentaire en entrant NET HELPMSG 2185.</pre>	
Net stop service	<pre>C:\Users\uti029&gt;Net start service Le nom de service n'est pas valide.  Vous obtiendrez une aide supplémentaire en entrant NET HELPMSG 2185.</pre>	

## 2 : Résolution de problème et suivi de connectivité :

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

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

<pre>C:\&gt;ping 10.1.0.2  Pinging 10.1.0.2 with 32 bytes of data:  Reply from 10.100.100.6: Destination host unreachable. Reply from 10.100.100.6: Destination host unreachable. Reply from 10.100.100.6: Destination host unreachable. Reply from 10.100.100.6: Destination host unreachable.  Ping statistics for 10.1.0.2:     Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)</pre>	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 :

<pre>C:\&gt;tracert 10.1.0.2  Tracing route to 10.1.0.2 over a maximum of 30 hops:    0  0 ms    0 ms    1 ms    10.0.0.254   1  1 ms    0 ms    0 ms    10.100.100.2   2  1 ms    0 ms    1 ms    10.100.100.6   3  1 ms    *        1 ms    10.100.100.6   4  *        1 ms    *        Request timed out.   5  1 ms           *   6  1 ms           *  Control-C ^C</pre>	La première adresse IP 10.0.0.254 appartient à GigabitEthernet 0/0
<pre>RouterA#show ip interface brief  Interface    IP-Address      OK? Method Status  Protocol GigabitEthernet0/0  10.0.0.254      YES manual up      up GigabitEthernet0/1  unassigned      YES unset  administratively down down GigabitEthernet0/2  unassigned      YES unset  administratively down down Serial0/0/0        10.100.100.1    YES manual up      up Serial0/0/1        unassigned      YES unset  administratively down down Vlan1             unassigned      YES unset  administratively down down</pre>	L'interface GigabitEthernet 0/0 représente des ports physiques par lesquels le périphérique est connecté à d'autres appareils du réseau.

```

C:\>tracert 10.1.0.2

Tracing route to 10.1.0.2 over a maximum of 30 hops:

  0  0 ms    0 ms    0 ms    10.0.0.254
  1  0 ms    0 ms    0 ms    10.100.100.2
  2  2 ms    2 ms    1 ms    10.100.100.6
  3  2 ms    *      0 ms    10.100.100.6
  4  2 ms    *      0 ms    10.100.100.6
  5  *      1 ms    *      Request timed out.
  6  1 ms    *      0 ms    10.100.100.6
  7  *      0 ms    *      Request timed out.
  8  2 ms    *      2 ms    10.100.100.6
  9  *      2 ms    *      Request timed out.
 10  1 ms    *      1 ms    10.100.100.6
 11  *      1 ms    *      Request timed out.
 12  2 ms    *      1 ms    10.100.100.6
 13  *      2 ms    *      Request timed out.
 14  2 ms    *      1 ms    10.100.100.6
 15  *      0 ms    *      Request timed out.
 16  20 ms   *      2 ms    10.100.100.6
 17  *      1 ms    *      Request timed out.
 18  2 ms    *      0 ms    10.100.100.6
 19  *      2 ms    *      Request timed out.
 20  12 ms   *      2 ms    10.100.100.6
 21  *      1 ms    *      Request timed out.
 22  2 ms    *      2 ms    10.100.100.6
 23  *      1 ms    *      Request timed out.
 24  2 ms    *      1 ms    10.100.100.6
 25  *      2 ms    *      Request timed out.
 26  1 ms    *      3 ms    10.100.100.6
 27  *      2 ms    *      Request timed out.
 28  2 ms    *      2 ms    10.100.100.6
 29  *      0 ms    *      Request timed out.
 30  1 ms    *      2 ms    10.100.100.6

```

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 ont des adresses entourant la dernière de la commande tracert : 10.100.100.4 < 1.100.100.6 < 1.100.100.8.

b)

```

RouterC#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
Serial0/0/0       10.100.100.17   YES manual up        up
Serial0/0/1       10.100.100.6    YES manual up        up
Vlan1             unassigned      YES unset  administratively down down

```

Les interfaces sont actives.

Dans ce sens ça fonctionne

Mais dans ce sens il y a un problème

Simulation Panel

Vis	Time(sec)	Last Device	At Device	Type
0.000	—	PC0	PC0	IC
0.000	—	PC0	PC3	IC
0.001	—	PC0	Switch1	IC
0.001	—	PC3	Switch2	IC
0.002	—	Switch1	RouterA	IC
0.002	—	Switch2	RouterD	IC
0.003	—	RouterA	RouterB	IC
0.003	—	RouterD	RouterC	IC
0.004	—	RouterB	RouterC	IC
0.004	—	RouterC	RouterB	IC
0.004	—	RouterC	RouterC	IC
0.005	—	RouterC	RouterB	IC
0.005	—	RouterB	RouterA	IC
0.006	—	RouterB	RouterA	IC
0.006	—	RouterA	Switch1	IC
0.007	—	RouterA	Switch1	IC
0.007	—	Switch1	PC0	IC
0.008	—	PC0	Switch1	IC
0.008	—	Switch1	RouterA	IC
0.009	—	RouterA	RouterB	IC
0.010	—	RouterB	RouterC	IC
0.011	—	RouterC	RouterB	IC

Reset Simulation ☒ Constant Delay

Play Controls

Event List Filters - Visible Events

ACL Filter: ARP, BGP, CDP, DHCP, DHCPv6, DNS, DTP, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTP, ICMPv6, IPsec, ISAKMP, LACP, NTP, OSPF, OSPFv6, PAP, POP3, RADIUS, RIP, RIPng, RTP, SCCP, SMTP, SSH, STP, SYSLOG, TACACS, TFTP, Telnet, UDP, VTP

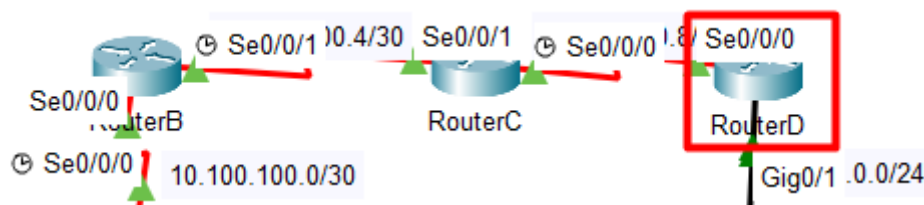
Time: 00:06:52.548

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

<p>PDU Information at Device: RouterC</p> <p>OSI Model    Inbound PDU Details</p> <p>At Device: RouterC Source: PC3 Destination: PC0</p> <table border="1"> <thead> <tr> <th>In Layers</th> <th>Out Layers</th> </tr> </thead> <tbody> <tr><td>Layer7</td><td>Layer7</td></tr> <tr><td>Layer6</td><td>Layer6</td></tr> <tr><td>Layer5</td><td>Layer5</td></tr> <tr><td>Layer4</td><td>Layer4</td></tr> <tr><td>Layer3: IP Header Src. IP: 10.0.0.1, Dest. IP: 10.1.0.2 ICMP Message Type: 0</td><td>Layer3:</td></tr> <tr><td>Layer2: HDLC Frame HDLC</td><td>Layer2</td></tr> <tr><td>Layer1: Port Serial0/0/1</td><td>Layer1</td></tr> </tbody> </table> <p>1. The device looks up the destination IP address in the CEF table. 2. The CEF table does not have an entry for the destination IP address. 3. The device looks up the destination IP address in the routing table.</p>	In Layers	Out Layers	Layer7	Layer7	Layer6	Layer6	Layer5	Layer5	Layer4	Layer4	Layer3: IP Header Src. IP: 10.0.0.1, Dest. IP: 10.1.0.2 ICMP Message Type: 0	Layer3:	Layer2: HDLC Frame HDLC	Layer2	Layer1: Port Serial0/0/1	Layer1	<p>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.</p>
In Layers	Out Layers																
Layer7	Layer7																
Layer6	Layer6																
Layer5	Layer5																
Layer4	Layer4																
Layer3: IP Header Src. IP: 10.0.0.1, Dest. IP: 10.1.0.2 ICMP Message Type: 0	Layer3:																
Layer2: HDLC Frame HDLC	Layer2																
Layer1: Port Serial0/0/1	Layer1																

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) :

<pre>interface Serial10/0/0  ip address 10.100.100.17 255.255.255.252  clock rate 64000 ! interface Serial10/0/1  ip address 10.100.100.6 255.255.255.252</pre>	<p>Les masques de sous-réseau Serials (les câbles utilisés) sont bons.</p> <p>L'adresse IP de Serial0/0/0 n'est pas bonne, comme elle est reliée au routerD.</p>
---	--

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

<pre>RouterC(config)#interface serial0/0/0 RouterC(config-if)#ip address 10.100.100.9 255.255.255.252 RouterC(config-if)#no shutdown</pre>	<p>10.100.100.9 au lieu de 10.100.100.17</p>
--	--

<pre>C:\&gt;tracert 10.1.0.2  Tracing route to 10.1.0.2 over a maximum of 30 hops:    1  1 ms    0 ms    0 ms    10.0.0.254   2  0 ms    1 ms    0 ms    10.100.100.2   3  0 ms    2 ms   28 ms    10.100.100.6   4  2 ms    2 ms    2 ms    10.100.100.10   5  0 ms    1 ms    0 ms    10.1.0.2  Trace complete.</pre>	<p>La commande tracert et l'enveloppe ICMP marchent et arrivent au PC3</p>
---	--







1

Test

New

Delete

Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Color
	Successful	PC0	PC3	ICMP	
	Successful	PC3	PC0	ICMP	
	Successful	PC0	PC3	ICMP	

2.4 : Comparer tracert avec traceroute sur un routeur :

<pre>RouterA&gt;traceroute 10.1.0.2 Type escape sequence to abort. Tracing the route to 10.1.0.2   1  10.100.100.2    0 msec    0 msec    2 msec  2  10.100.100.6   42 msec   3 msec   37 msec  3  10.100.100.10  1 msec    25 msec  1 msec  4  10.1.0.2       15 msec   3 msec   2 msec</pre>	Ca fonctionne bien car la dernière adresse est celle de PC3.
<pre>C:\&gt;tracert 10.1.0.2  Tracing route to 10.1.0.2 over a maximum of 30 hops:   0  0 ms    0 ms    0 ms    10.0.0.254  1  0 ms    1 ms    0 ms    10.100.100.2  2  0 ms    2 ms   28 ms   10.100.100.6  3  2 ms    2 ms    2 ms   10.100.100.10  4  0 ms    1 ms    0 ms   10.1.0.2</pre>	<pre>RouterA&gt;traceroute 10.1.0.2 Type escape sequence to abort. Tracing the route to 10.1.0.2   1  10.100.100.2    0 msec    0 msec    2 msec  2  10.100.100.6   42 msec   3 msec   37 msec  3  10.100.100.10  1 msec    25 msec  1 msec  4  10.1.0.2       15 msec   3 msec   2 msec RouterA&gt;</pre>

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)

<pre>RouterA#traceroute 10.1.0.2 Type escape sequence to abort. Tracing the route to 10.1.0.2   1  10.100.100.2    6 msec    5 msec    3 msec  2  10.100.100.6   3 msec    7 msec    9 msec  3  10.100.100.10  6 msec    3 msec   16 msec  4  10.1.0.2       7 msec    5 msec   10 msec  RouterA#extended traceroute ^ % Invalid input detected at '^' marker.</pre>	La commande extended traceroute, entrée dans le mode privilégié n'est pas reconnu. Il faut juste utiliser la commande traceroute dans le mode privilégié.
<pre>RouterA#traceroute Protocol [ip]: ip Target IP address: 10.1.0.2 Source address: 10.100.100.1 Numeric display [n]: n Timeout in seconds [3]: 3 Probe count [3]: 5 Minimum Time to Live [1]: 1 Maximum Time to Live [30]: 30 Type escape sequence to abort. Tracing the route to 10.1.0.2   1  10.100.100.2    3 msec    7 msec    0 msec    6 msec    5 msec  2  10.100.100.6    5 msec    9 msec    8 msec    6 msec   10 msec  3  10.100.100.10  17 msec    9 msec   13 msec    9 msec    0 msec  4  10.1.0.2        9 msec    3 msec   15 msec    6 msec    0 msec</pre>	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)

<pre>Probe count [3]: 5 Minimum Time to Live [1]: 1 Maximum Time to Live [30]: 30 Type escape sequence to abort. Tracing the route to 10.1.0.2   1  10.100.100.2    3 msec    7 msec    0 msec    6 msec    5 msec  2  10.100.100.6    5 msec    9 msec    8 msec    6 msec   10 msec  3  10.100.100.10  17 msec    9 msec   13 msec    9 msec    0 msec  4  10.1.0.2        9 msec    3 msec   15 msec    6 msec    0 msec RouterA#</pre>	5 paquets ICMP sont envoyés à chaque saut, comme défini (Probe count). Routeur A a envoyé 5*4, donc 20 paquets.
--	--

c)

<pre>RouterA#traceroute Protocol [ip]: ip Target IP address: 10.1.0.2 Source address: 10.100.100.1 Numeric display [n]: n Timeout in seconds [3]: 7 Probe count [3]: 5 Minimum Time to Live [1]: 1 Maximum Time to Live [30]: 30 Type escape sequence to abort. Tracing the route to 10.1.0.2   1  10.100.100.2    4 msec    1 msec    0 msec    2 msec    2 msec  2  10.100.100.6    2 msec    10 msec   13 msec   12 msec    7 msec  3  10.100.100.10   12 msec    3 msec    8 msec    8 msec   17 msec  4  10.1.0.2        2 msec     1 msec     5 msec    3 msec   15 msec</pre>	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'à 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 :





<pre>RouterA&gt;enable RouterA#configure terminal Enter configuration commands, one per line. End with CNTL/Z. RouterA(config)#router rip RouterA(config-router)#version 2 RouterA(config-router)#network 10 RouterA(config-router)#network 10.0.0.0 RouterA(config-router)#network 10.100.100.0</pre>	<p>3 : activer le processus de routage RIP.</p> <p>4 : définit la version de RIP à utiliser (le RIP1 est par default)</p> <p>5 : activer le routage pour le réseau 10.0.0.0</p> <p>6 : activer le routage pour le réseau 10.100.100.0</p>
--	---

Les commandes en grises sont à 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 :

	Successful	PC1	PC3	ICMP		0.000	N	0	(edit)
	Successful	PC3	PC1	ICMP		14.930	N	1	(edit)

## 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](#)

[Loopback — Wikipédia](#)