

# LABO 3 B-3

25/09/2023

*Protocoles DHCP et DNS*

**I. Table des matières**

I.	Table des matières.....	2
II.	Tableau de Suivi des Modifications :.....	3
III.	Introduction .....	4
IV.	Script bat.....	4
	a) Intérêt script bat .....	4
	b) Script python.....	5
	c) Fonctionnement sous linux : .....	8
V.	Ping.....	8
VI.	Fonctionnement des TTL .....	9
	d) RFC TTL : .....	10
	e) Valeur des ttl.....	10
VII.	Analyse de trame : .....	11
	f) Méthode d'OSINT passif .....	11
VIII.	Traceroute .....	16
IX.	Fichier host et association réseaux : .....	19
X.	Simulation empoisonnement SEO : .....	24
XI.	TTL : .....	26
XII.	Arp .....	26
	g) Réseaux locaux : .....	28
XIII.	Machine virtuelle : .....	28
	h) Outils arp sous linux : .....	33
XIV.	Analyse web .....	33
XV.	Route : .....	36
XVI.	NetSH.....	38
	i) Réinitialisation de la pile IP .....	40
	j) Commande d'analyse .....	40
	k) Analyse des communications : .....	42
XVII.	Netstat : .....	44
	l) Pour obtenir les statistiques d'utilisation d'Ethernet .....	45
	m) Les noms des fichiers exécutables impliqués dans la création de la connexion .....	47
XVIII.	Etape Bonus NMAP : .....	49
XIX.	Packet tracer .....	54
XX.	Routage dynamique : .....	57
XXI.	Conclusion : .....	58

XXII.	Annexe : .....	59
n)	Commande à retenir .....	59
o)	Protocoles vus .....	60
p)	Langage abordé.....	61
q)	Librairie : .....	61
XXIII.	Sources : .....	62

## II. Tableau de Suivi des Modifications :

Date	Auteur	Description des modifications :
12/11/2023	Eloham	Analyse du dossier, choix des bibliothèques qui seront utiles pour le projet
13/11/2023	Eloham	Mise en place d'une analyse OSINT
14/11/2023	Eloham	Utilisation de l'outil traceroute
15/11/2023	Eloham	Configuration du fichier hosts via Python
16/11/2023	Eloham	TTL et dns
17/11/2023	Eloham	Analyse ARP
19/11/2023	Eloham	Machine virtuelle Kali Linux
21/11/2023	Eloham	Mise en place des routes et analyse Netsh
22/11/2023	Eloham	Analyse réseau avec Netsh
23/11/2023	Eloham	Développement du rapport
24/11/2023	Eloham	Création des scripts finaux
30/11/2023	Eloham	Nmap Bonus
03/12/2023	Eloham	Packet tracer



### III. Introduction

Cet atelier s'inscrit dans le cadre du DevOps et se concentrera sur les méthodes de surveillance des réseaux en utilisant du code en ligne. Nous devons appliquer une méthodologie d'OSINT en utilisant des scripts en batch ou en Python pour analyser notre environnement, ainsi que différents sites revêtant une importance majeure dans le domaine de l'informatique.

### IV. Script bat

Un script batch, ou fichier de commandes batch, est un fichier texte contenant une séquence de commandes système. Son objectif principal est d'automatiser l'exécution de tâches répétitives sur un système d'exploitation Windows. Les scripts batch peuvent être utilisés pour lancer des programmes, copier des fichiers, créer des répertoires, et effectuer d'autres opérations systèmes.

#### a) Intérêt script bat

L'intérêt majeur des scripts batch réside dans leur capacité à automatiser des processus sans intervention manuelle constante. Cela permet d'économiser du temps et d'assurer une exécution cohérente des tâches. Les scripts batch existent depuis les premières versions de MS-DOS dans les années 1980, et ils sont toujours largement utilisés pour la gestion de systèmes et l'automatisation de tâches système.

On peut créer des scripts pour automatiser certaines tâches. Voici un exemple :

```
C:\Users\eloha\Desktop\TP4 DROGUE\Sript.bat - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help

Sript.bat x import shodan @echo off drogue_booster.pyw Eloham_caronDSN3.java utilise les librairie tkinter et socket script1.bat python.py

1 @echo off
2 echo "Déterminez si le serveur distant est accessible."
3 echo "Déterminez si le serveur distant est accessible." >> Analyse.txt
4 ping -4 cisco.com
5 ping -4 cisco.com >> Analyse.txt
6 ping -6 cisco.com
7 ping -6 cisco.com >> Analyse.txt
8
9 echo "Test V4"
10 echo "Test V4" >> Analyse.txt
11 echo "Organismes principaux d'Internet"
12 echo "Organismes principaux d'Internet" >> Analyse.txt
13 ping -4 www.afnic.net
14 ping -4 www.afnic.net >> Analyse.txt
15 ping -4 www.apnic.net
16 ping -4 www.apnic.net >> Analyse.txt
17 ping -4 www.ripe.net
18 ping -4 www.ripe.net >> Analyse.txt
19 ping -4 www.lacnic.net
20 ping -4 www.lacnic.net >> Analyse.txt
21 ping -4 www.arin.net
22 ping -4 www.arin.net >> Analyse.txt
23
24 echo "Test V6"
25 echo "Test V6" >> Analyse.txt
26 ping -6 www.afnic.net
27 ping -6 www.afnic.net >> Analyse.txt
28 ping -6 www.apnic.net
29 ping -6 www.apnic.net >> Analyse.txt
30 ping -6 www.ripe.net
31 ping -6 www.ripe.net >> Analyse.txt
32 ping -6 www.lacnic.net
33 ping -6 www.lacnic.net >> Analyse.txt
34 ping -6 www.arin.net
35 ping -6 www.arin.net >> Analyse.txt
36
37 echo "Suivre une route vers un serveur distant à l'aide de la commande Tracert"
38 echo "Suivre une route vers un serveur distant à l'aide de la commande Tracert" >> Analyse.txt
39 tracert www.cisco.com
40 tracert www.cisco.com >> Analyse.txt
41 tracert peugeot.fr
42 tracert peugeot.fr >> Analyse.txt
43 tracert sfr.fr
44 tracert sfr.fr >> Analyse.txt
45 tracert cisco.fr
46 tracert cisco.fr >> Analyse.txt
47 tracert -h 5 google.com
48 tracert -h 5 google.com >> Analyse.txt
49
50 echo "curl -s http://ping.eu/"
51 echo "curl -s http://ping.eu/" >> Analyse.txt
52 curl -s http://ping.eu/
53 curl -s http://ping.eu/ >> Analyse.txt
54 echo "curl -s http://www.subnetonline.com/pages/network-tools/online-tracepath.php"
55 echo "curl -s http://www.subnetonline.com/pages/network-tools/online-tracepath.php" >> Analyse.txt

Line 8, Column 1
```

Le problème avec ce type de script réside dans son interface peu esthétique et illisible, surtout pour une personne débutante en informatique.

```
C:\WINDOWS\system32\cmd. x + v
"D|@terminez si le serveur distant est accessible."

Envoi d'une requête 'ping' sur cisco.com [72.163.4.185] avec 32 octets de données :
Réponse de 72.163.4.185 : octets=32 temps=125 ms TTL=238
Réponse de 72.163.4.185 : octets=32 temps=125 ms TTL=238
```

De plus, si l'on souhaite utiliser des outils complémentaires, nous sommes limités. Bien que des outils tels que Nmap, Metasploit, et d'autres outils d'hacking soient disponibles, le terminal Linux offre une bien meilleure expérience dans ce contexte.

## b) Script python

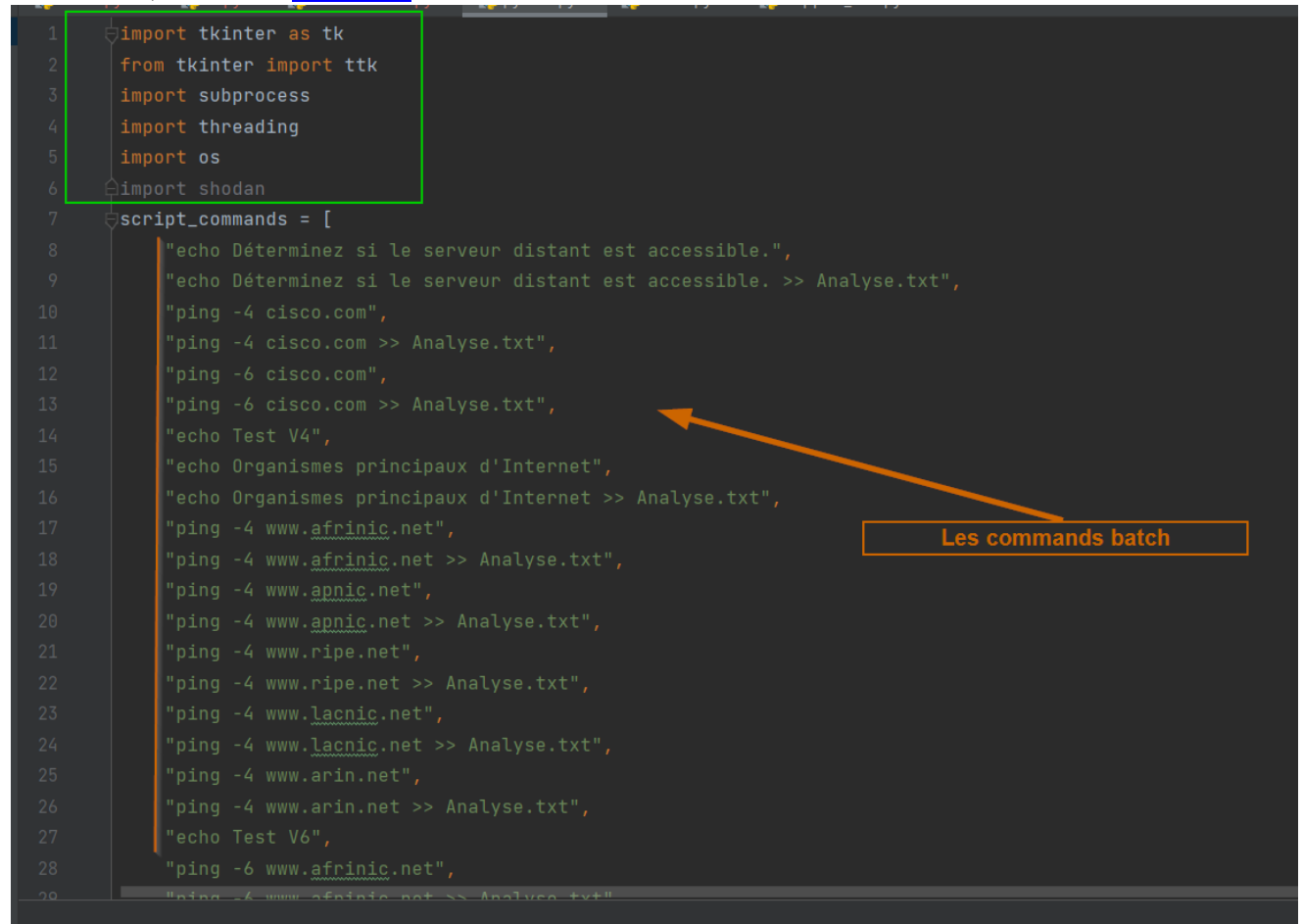
Pour ma part, j'ai choisi d'opter pour des méthodes plus modernes, telles que Python. C'est un langage largement supérieur pour le scripting, car il permet d'intégrer des API telles que Shodan, Nmap, Tkinter pour l'ajout d'interfaces graphiques, ainsi que des modules socket pour la communication. De plus, Python est compatible avec tous les systèmes d'exploitation, et il est installé par défaut sur macOS et Linux.

Par exemple, on peut intégrer Shodan.

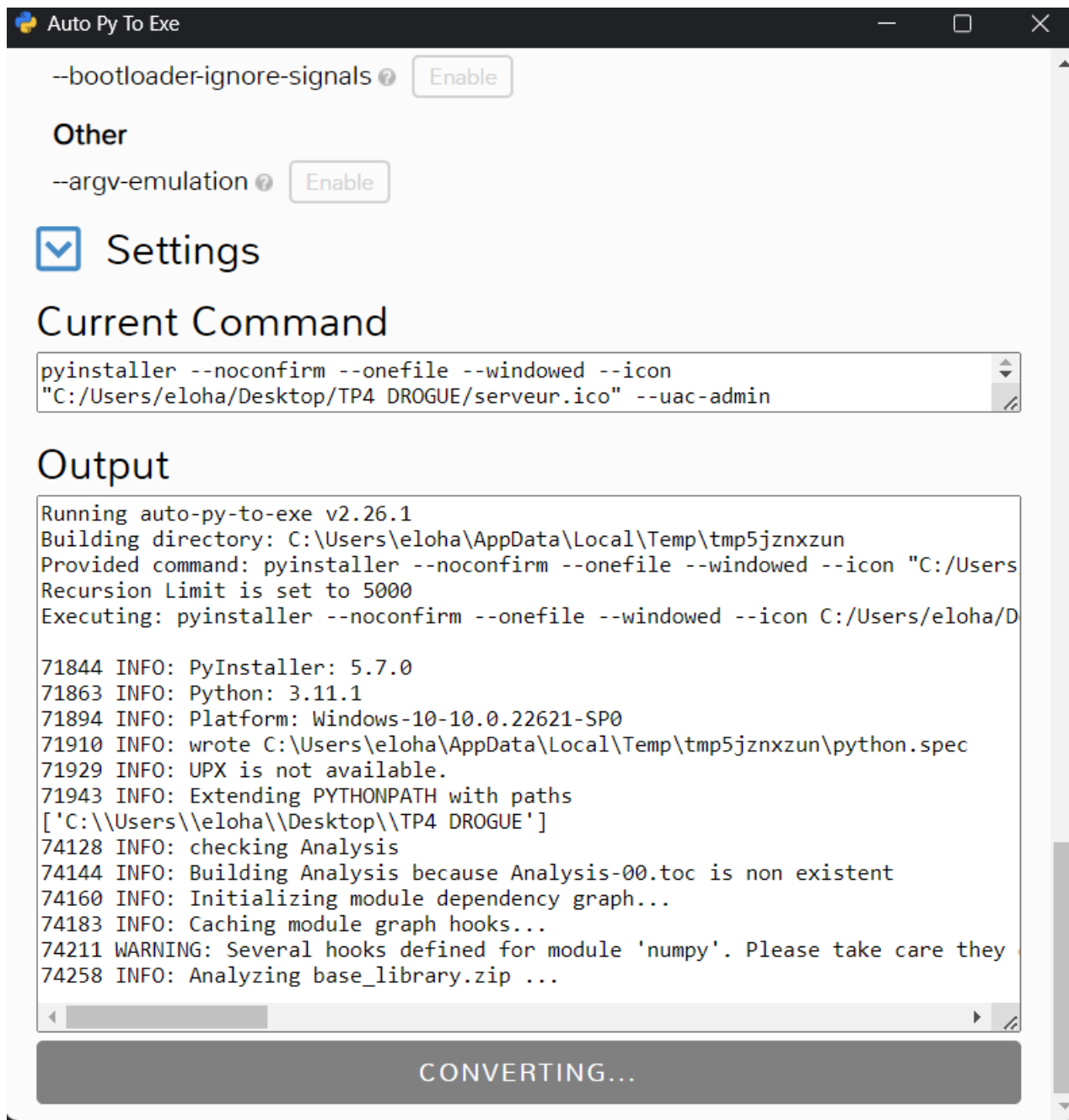
```
C:\Users\eloha>pip install shodan
Defaulting to user installation because normal site-packages is not writeable
DEPRECATION: Loading egg at c:\program files\python311\lib\site-packages\vbboxapi-1.0-py3.11.egg is deprecated. pip 24.3
will enforce this behaviour change. A possible replacement is to use pip for package installation.. Discussion can be fo
und at https://github.com/pypa/pip/issues/12330
Collecting shodan
  Downloading shodan-1.30.1.tar.gz (57 kB)
    ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 57.9/57.9 kB 1.5 MB/s eta 0:00:00
  Installing build dependencies ... done
  Getting requirements to build wheel ... done
  Preparing metadata (pyproject.toml) ... done
Requirement already satisfied: click in c:\users\eloha\appdata\roaming\python\python311\site-packages (from shodan) (8.1
.3)
Collecting click-plugins (from shodan)
  Downloading click_plugins-1.1.1-py2.py3-none-any.whl (7.5 kB)
Requirement already satisfied: colorama in c:\users\eloha\appdata\roaming\python\python311\site-packages (from shodan) (
```

Il est crucial d'inclure les bibliothèques nécessaires. Les détails se trouvent à la fin du document, dans les [annexes](#).

```
1 import tkinter as tk
2     from tkinter import ttk
3     import subprocess
4     import threading
5     import os
6     import shodan
7     script_commands = [
8         "echo Déterminez si le serveur distant est accessible.",
9         "echo Déterminez si le serveur distant est accessible. >> Analyse.txt",
10        "ping -4 cisco.com",
11        "ping -4 cisco.com >> Analyse.txt",
12        "ping -6 cisco.com",
13        "ping -6 cisco.com >> Analyse.txt",
14        "echo Test V4",
15        "echo Organismes principaux d'Internet",
16        "echo Organismes principaux d'Internet >> Analyse.txt",
17        "ping -4 www.afrinic.net",
18        "ping -4 www.afrinic.net >> Analyse.txt",
19        "ping -4 www.apnic.net",
20        "ping -4 www.apnic.net >> Analyse.txt",
21        "ping -4 www.ripe.net",
22        "ping -4 www.ripe.net >> Analyse.txt",
23        "ping -4 www.lacnic.net",
24        "ping -4 www.lacnic.net >> Analyse.txt",
25        "ping -4 www.arin.net",
26        "ping -4 www.arin.net >> Analyse.txt",
27        "echo Test V6",
28        "ping -6 www.afrinic.net",
29        "ping -6 www.afrinic.net >> Analyse.txt"
```



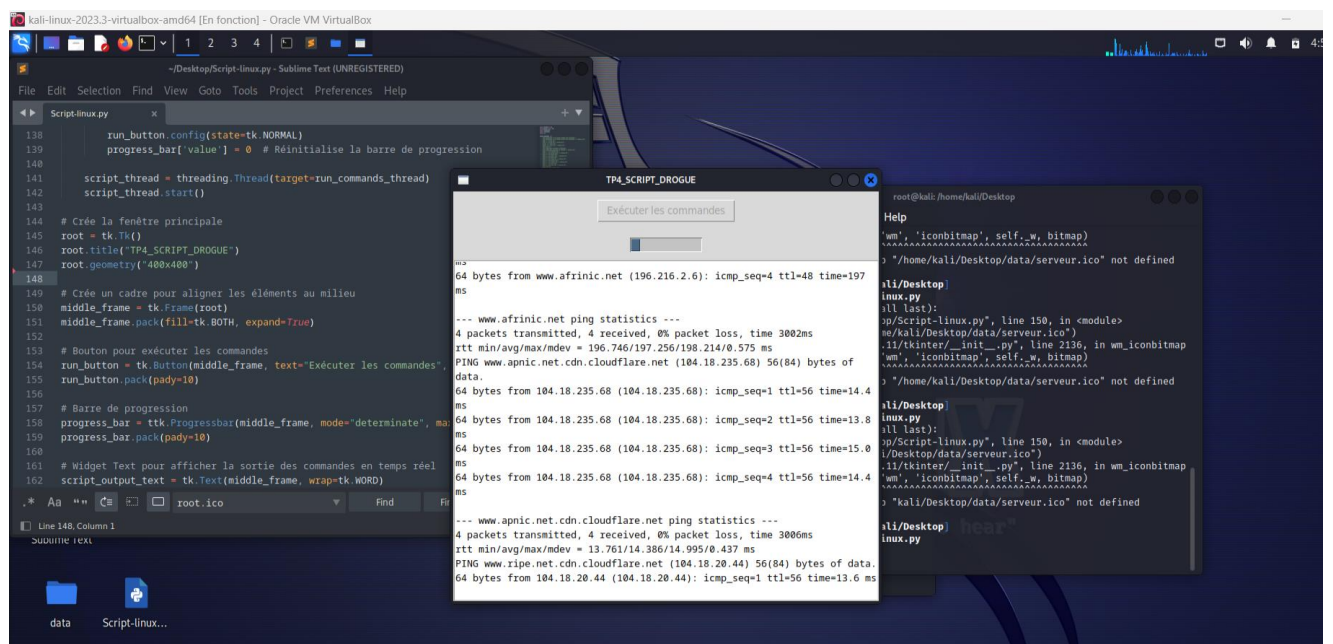
Les commands batch



On peut le convertir en fichier exécutable (exe) afin de le rendre plus accessible pour des utilisateurs ordinaires.



### c) Fonctionnement sous linux :



J'ai dû retirer l'icône car elle était mal interprétée par le terminal Linux.

## V. Ping

Les 4 server bloque les trame icmpV6

Pour l'Afrique : ping [www.afnic.net](http://www.afnic.net)

Pour l'Australie : ping [www.apnic.net](http://www.apnic.net)

Pour l'Europe : ping [www.ripe.net](http://www.ripe.net)



Pour l'Amérique du Sud : ping [www.lacnic.net](http://www.lacnic.net)

Le dernier bloc les trame icmp tout cour

Pour l'Amérique : ping [www.arin.net](http://www.arin.net)

```
PS C:\Users\eloha> tracert www.arin.net

Détermination de l'itinéraire vers www.arin.net [199.43.0.47]
avec un maximum de 30 sauts :

  1    2 ms    1 ms    2 ms  lanspeedtest.wifirst.fr [10.188.0.1]
  2    2 ms    2 ms    2 ms  172.22.4.1
  3   13 ms   10 ms    8 ms  192.168.255.1
  4   13 ms   12 ms   12 ms  172.21.18.246
  5   26 ms    *      *    port-channel12.core2.par2.he.net [184.104.19
6.230]
  6    *      *      *    Délai d'attente de la demande dépassé.
  7   91 ms   89 ms   89 ms  arin.10gigabitethernet1-3.core1.ash1.he.net
[216.66.36.18]
  8   90 ms   90 ms   90 ms  host-199-43-0-194.arin.net [199.43.0.194]
  9    *      *      *    Délai d'attente de la demande dépassé.
 10    *      *      *    Délai d'attente de la demande dépassé.
 11    *      *      *    Délai d'attente de la demande dépassé.
 12    *      *      *    Délai d'attente de la demande dépassé.
 13
```

Figure 1 Analyse arin.net

le pare feu bloquant les trame ne se trouve pas directement a l'entrée du réseaux comme vue cis dessous

## VI. Fonctionnement des TTL

```
tracert www.cisco.com
tracert peugeot.fr
tracert sfr.fr
tracert cisco.fr
```

Figure 2 Analyse ttl

Les valeurs de TTL (Time-To-Live) dans les résultats d'un tracert peuvent varier en raison de la manière dont les routeurs gèrent les paquets. Le TTL est un champ dans l'en-tête d'un paquet IP qui spécifie le nombre de sauts qu'un paquet peut faire avant d'être abandonné.

Lorsqu'un paquet traverse un routeur, le routeur décrémente la valeur TTL de ce paquet. Si le TTL atteint zéro, le paquet est abandonné, et le routeur envoie un message ICMP "Time Exceeded" au point d'origine du paquet. Ce processus est utilisé pour éviter que les paquets ne circulent indéfiniment s'il y a un problème dans le réseau.

Maintenant, pourquoi les valeurs de TTL peuvent varier :

- Longueur du chemin : Chaque route entre le point d'origine et la destination décrémente le TTL. Si le chemin vers un serveur est plus long que celui vers un autre, les valeurs de TTL seront différentes.

- Politiques de routage : Certains routeurs peuvent être configurés pour décrémenter le TTL de manière différente. Par exemple, un administrateur réseau peut choisir de décrémenter le TTL de plusieurs sauts à la fois.
- Charge réseau : Si un réseau est surchargé, des routeurs peuvent choisir des chemins alternatifs qui peuvent avoir des longueurs différentes, ce qui affecte les valeurs de TTL.

En résumé, les variations dans les valeurs de TTL sont normales en raison des différents chemins que les paquets peuvent emprunter à travers le réseau et des politiques de routage mises en place.

#### **d) RFC TTL :**

La RFC (Request for Comments) qui spécifie des recommandations concernant la valeur TTL (Time-To-Live) est la RFC 791, intitulée "Internet Protocol" (IP). Cette RFC définit le format des en-têtes IP, y compris le champ TTL.

Les RFC sont émises par l'Internet Engineering Task Force (IETF), qui est une organisation qui développe et promeut les normes Internet. Les RFC sont des documents de spécifications techniques qui décrivent divers aspects des protocoles Internet, des normes et des bonnes pratiques.

Il est important de noter que les RFC ne sont pas des lois, et leur respect n'est pas obligatoire d'un point de vue légal. Cependant, dans la pratique, de nombreuses normes et protocoles Internet reposent sur ces spécifications, et leur adoption est largement suivie pour assurer l'interopérabilité des systèmes et des réseaux.

Ainsi, bien que les RFC ne soient pas juridiquement contraignantes, leur adoption volontaire est généralement considérée comme une meilleure pratique pour garantir une cohérence et une compatibilité au sein de l'écosystème Internet.

#### **e) Valeur des ttl**

Ma valeur par défaut utilisé par l'ordinateur est de 30. Cela signifie que chaque paquet IP est initialement configuré avec un TTL de 30, et cette valeur est décrémentée à chaque saut à travers les routeurs du réseau. Si la valeur atteint zéro, le routeur envoie un message ICMP "Time Exceeded" à la source.

## VII. Analyse de trame :

L'adresse IP 81.253.184.86, qui apparaît dans le résultat de tracertr, est associée à Orange, un fournisseur d'accès à Internet (FAI). En particulier, cette adresse IP est probablement utilisée par un routeur ou un point de présence (POP) dans le réseau d'Orange, comme indiqué par les noms de domaine associés à chaque saut.

Il est important de noter que l'identification précise du propriétaire d'une adresse IP peut parfois être complexe, car les FAI peuvent avoir plusieurs adresses IP et leur infrastructure peut être partagée entre plusieurs services. Cependant, dans cet exemple, la présence des noms de domaine associés à Orange, tels que "rbc1.orange.net", indique une forte probabilité d'appartenance à Orange.

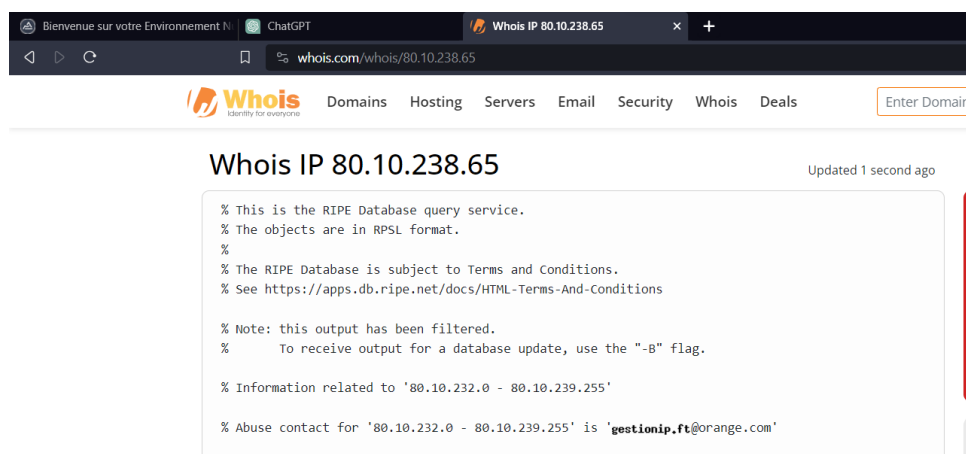


Figure 3 Identification de l'adresse 80.10.238.65

### f) Méthode d'OSINT passif

Whois peut être un outil très utile lorsqu'on souhaite obtenir des informations sur une adresse IP, son DNS, ou découvrir à qui appartient cette adresse IP. Cet outil permet d'explorer les détails liés à la propriété d'une adresse IP donnée. Par exemple, si l'on souhaite obtenir des informations sur le site web btssio.org, Whois permet de déterminer le propriétaire de ce site internet :

Registrant Contact	
Organization:	GDPR Masked
State:	Midi-Pyrenees
Country:	FR

Figure 4 propriétaire

Shodan est un moteur de recherche spécialisé dans la recherche d'appareils connectés à Internet. Contrairement aux moteurs de recherche classiques, Shodan se concentre sur l'exploration des dispositifs plutôt que sur le contenu des pages web. Il analyse les protocoles et les ports utilisés par ces dispositifs pour fournir des informations détaillées sur

les serveurs, les routeurs, les caméras de sécurité, les systèmes industriels, et bien d'autres.

L'intérêt, dans notre contexte, d'utiliser Shodan en complément d'outils tels que Whois réside dans la complémentarité des informations fournies par ces deux sources. Shodan vient compléter les lacunes laissées par Whois, et vice versa. En associant ces deux outils, on obtient une vision plus complète et approfondie des éléments recherchés, renforçant ainsi la précision et la pertinence des données recueillies.

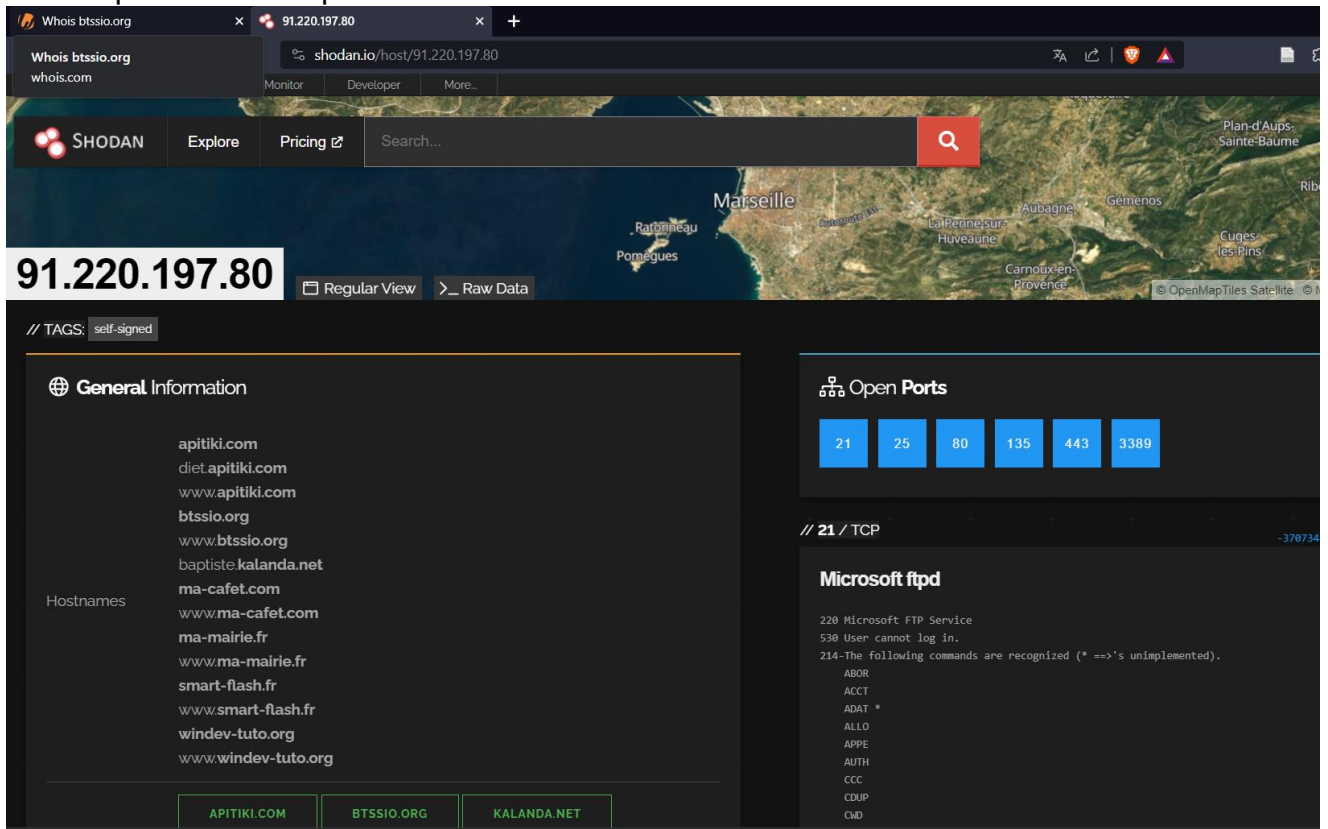


Figure 5 Outil shodan

Cela nous permet de voir que sur le server ou est héberger btssio.org il n'est pas le seul site web héberger dessus

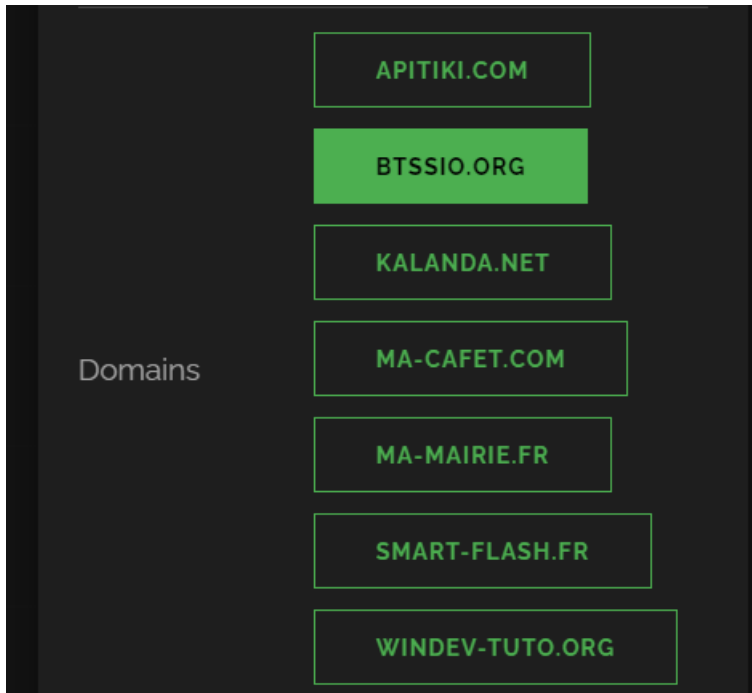


Figure 6 Protocoles associer

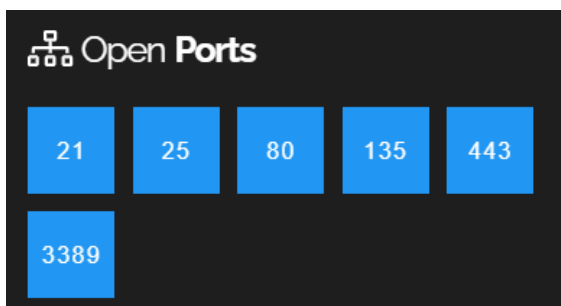


Figure 7 Détails des ports

En regardant dans les ports ouverts on se rend compte que l'outil Remote desktop est installé sur le serveur sur le port 3389.

Remote Desktop, similaire à des outils tels qu'**AnyDesk** et **TeamViewer**, facilite la connexion à distance à une machine afin d'en prendre le contrôle, sous réserve du consentement de l'utilisateur. Ces logiciels constituent des outils essentiels pour les techniciens réseau, leur permettant de résoudre des problèmes à distance. Dans le cas présent, il semble être utilisé comme un serveur FTP et SSH simultanément, offrant aux différents administrateurs de sites web la possibilité d'accéder à leurs sites et de les administrer à distance. Cette polyvalence en fait un élément clé pour la gestion efficace des systèmes informatiques à distance.

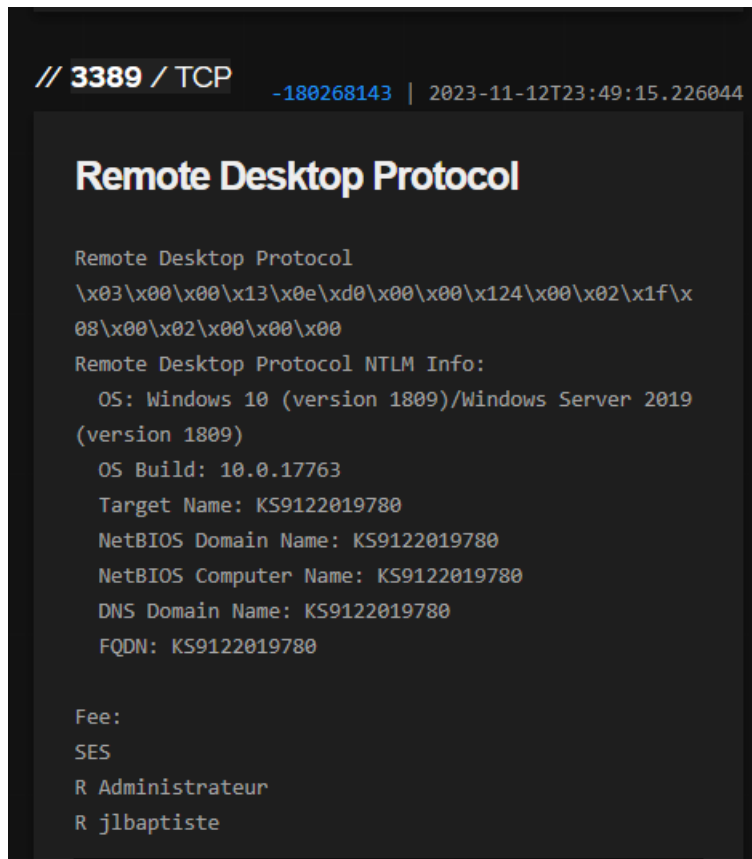


Figure 8 Remote desktop protocol

1

Sur le port 80 le service IIS qui héberge le serveur web :

Un serveur IIS, acronyme de Internet Information Services, est un serveur web développé par Microsoft. Il est utilisé pour héberger des sites web, des applications web et d'autres services en ligne. IIS prend en charge divers protocoles de communication, tels que HTTP, HTTPS, FTP, FTPS, SMTP, et plus encore.

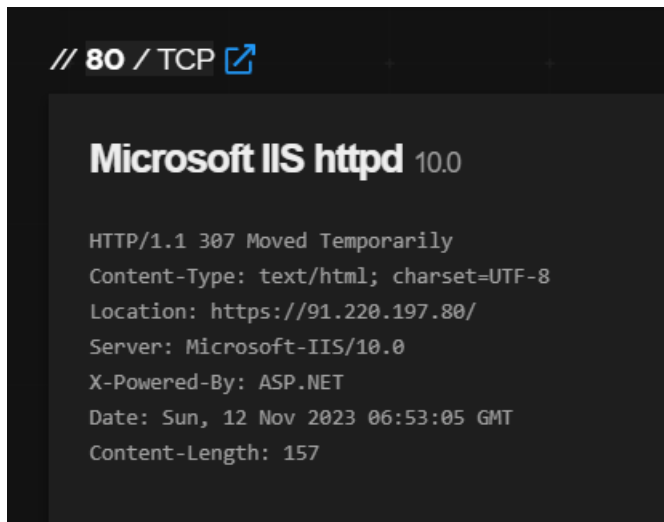


Figure 9 Server IIS

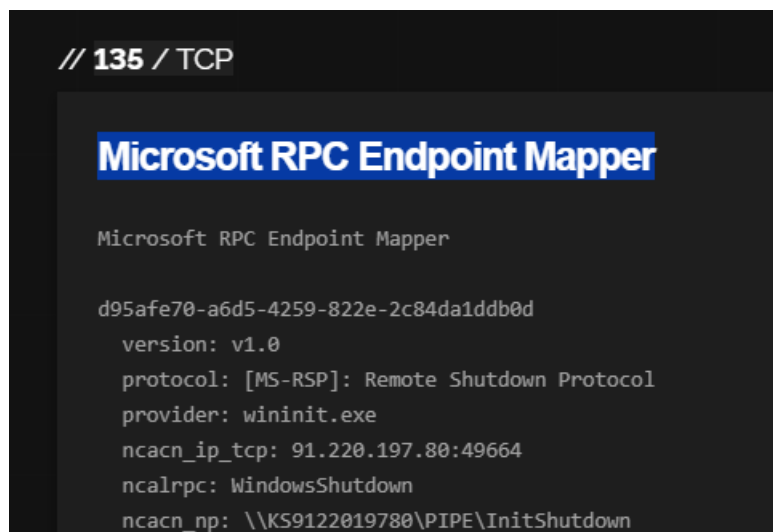


Figure 10 Rcp Endpoint Mapper

Le Microsoft RPC Endpoint Mapper (Gestionnaire de points de terminaison RPC) est un service qui fait partie du protocole RPC (Remote Procedure Call) sur les systèmes d'exploitation Microsoft Windows. Son rôle principal est de mapper ou d'associer des numéros de port aux services RPC sur un serveur.

Lorsqu'un client souhaite exécuter une procédure distante sur un serveur via RPC, il doit d'abord connaître le numéro de port sur lequel le service RPC nécessaire est en écoute. C'est là que le RPC Endpoint Mapper entre en jeu. Le client envoie une requête au Gestionnaire de points de terminaison RPC sur le serveur, demandant le numéro de port associé au service RPC spécifique.

Country	France
City	Marseille
Organization	SAS KALANDA
ISP	SAS KALANDA
ASN	AS61047
Operating System	Windows (build 10.0.17763)

Figure 11 Localisation Server

On observe que le serveur est hébergé en France, ce qui peut être intéressant pour une personne attentive au respect du RGPD et à la sécurité de ses données. Les serveurs hébergés en Europe et en France sont ceux qui respectent au mieux le règlement de la CNIL. C'est pourquoi cette information peut être pertinente.x

Toute cette analyse peut être pratique si l'on souhaite se faire recruter dans une entreprise on peut déjà analyse de l'extérieur les infos de l'entreprise se renseigner a l'avance et monter que nous somme intéresser et que nous connaissons déjà certain aspect de plus cela permet d'avoir un avantage sur la situation et de ce préparer a l'avance, et peut même procure un avantage psychologique certain lors du recrutement

## VIII. Traceroute

Une commande de type traceroute (ou tracert sur certains systèmes) est utilisée pour tracer le chemin suivi par les paquets de données entre l'ordinateur de l'utilisateur et un serveur distant. Elle permet d'identifier les étapes intermédiaires, appelées sauts, que les données parcourent à travers le réseau. Cette information est cruciale pour diagnostiquer des problèmes de connectivité, localiser des goulets d'étranglement, ou détecter des retards.

Dans le contexte de l'analyse d'un site internet, traceroute peut aider à déterminer les points de défaillance potentiels dans le réseau. Si un site est inaccessible ou présente des retards, traceroute peut identifier où le flux de données est interrompu ou ralenti. Cela permet aux professionnels de la cybersécurité et des réseaux, comme vous en tant que BTS SIO en cybersécurité réseaux, de cibler les problèmes et de les résoudre de manière efficace.



Aujourd'hui, je vais utiliser deux outils Web différents, <http://ping.eu/> et <http://www.subnetonline.com/pages/network-tools/online-tracepath.php>, pour effectuer un traceroute sur le site [www.afrinic.net](http://www.afrinic.net).

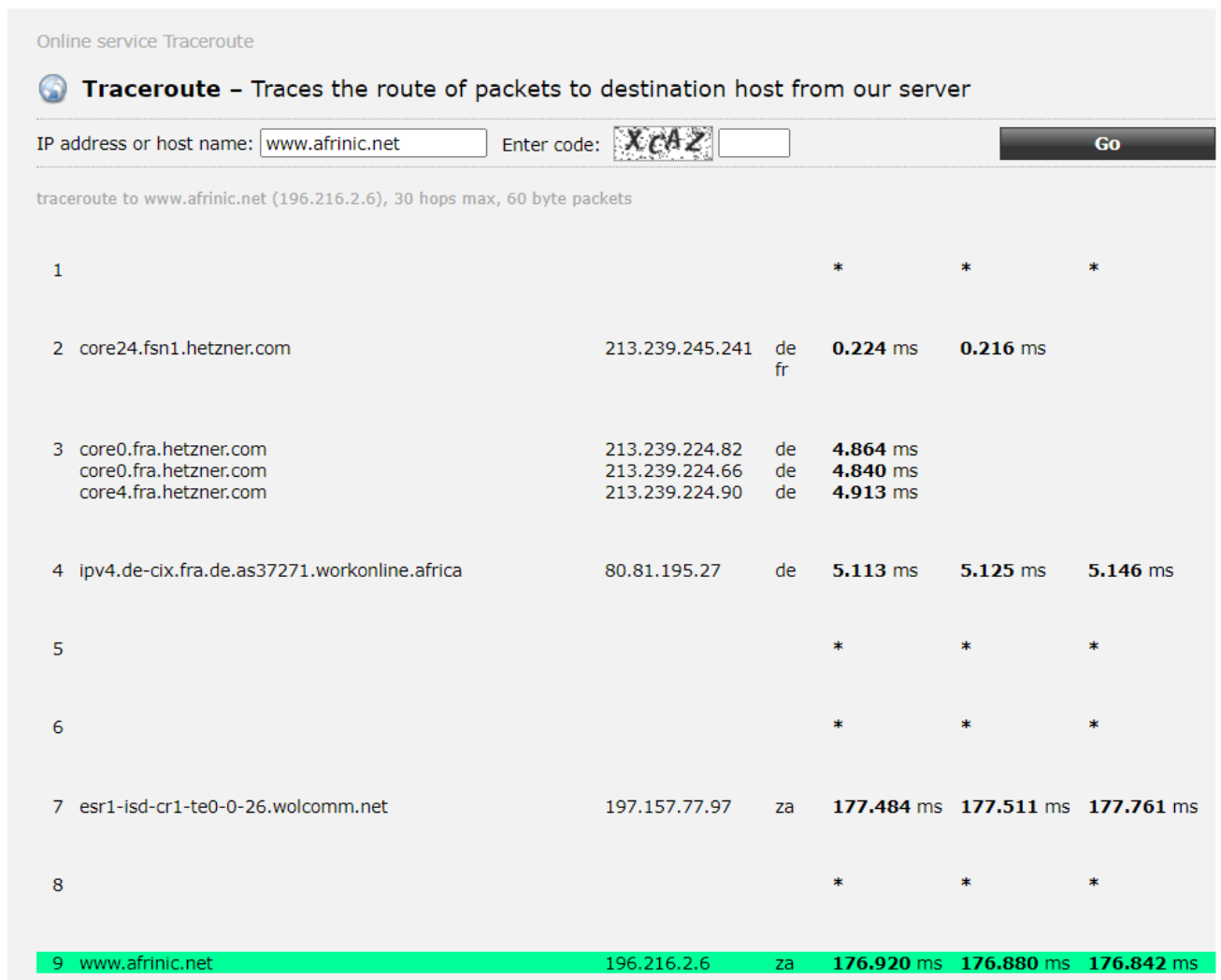


Figure 12 Traceroute afrinic

## ONLINE TRACEROUTE

**Traceroute** is a computer network tool used to determine the route taken by packets across an IP network.

The traceroute tool is available on practically all Unix-like operating systems. Variants with similar functionality are also available, such as tracepath on modern Linux installations and tracert on Microsoft Windows operating systems. Windows NT-based operating systems also provide pathping, which provides similar functionality.

Source: **Wikipedia**

An IPv6 version of this tool is **available here!**

Please be patient and wait for the task to finish!

TraceRoute Output:

traceroute to www.afrinic.net (196.216.2.6), 30 hops max, 60 byte packets

```
1 gw.giga-dns.com (91.194.90.1) 0.355 ms 0.335 ms 0.319 ms
2 gw02.giga-hosting.biz (213.248.101.77) 2.934 ms 2.919 ms 2.933 ms
3 * * *
4 ffm-b11-link.ip.twelve99.net (62.115.124.119) 6.153 ms 6.070 ms 6.157 ms
5 * * *
6 * * *
7 62.67.26.46 (62.67.26.46) 7.425 ms 7.319 ms 7.318 ms
8 * * *
9 * * *
10 esr1-isd-cr1-te0-0-26.wolcomm.net (197.157.77.97) 179.192 ms 179.182 ms 179.230 ms
11 197.157.64.195 (197.157.64.195) 178.733 ms 178.824 ms 178.708 ms
12 www.afrinic.net (196.216.2.6) 178.887 ms 178.788 ms 179.549 ms
```

## WHAT DOES THE OUTPUT OF ONLINE TRACEROUTE MEAN?

This online tool traces the route your packets follows from this webserver to any (reachable) destination on the internet. Enter the domain name or IP number of the webserver you want to test e.g., [www.yahoo.com](http://www.yahoo.com). Be patient, this script may take upto 60 seconds to return any results, it does not print out the lines one by one, just returns the whole traceroute.

Figure 13 Traceroute 2

L'analyse IPv6 est entravée en raison du fonctionnement du traceroute par trame ICMP. Dans les deux situations, les résultats sont pertinents, car le parcours emprunté n'est pas le même, étant donné que les serveurs d'origine diffèrent. Il peut être opportun d'explorer divers itinéraires afin de cibler précisément le problème, qu'il soit d'origine interne ou

Please be patient and wait for the task to finish!

TraceRoute IPv6 Output:  
---- Finished -----

externe.

Certaines des traceroutes peuvent contenir l'abréviation asymm. Cela fait référence à "asymmetric", qui signifie asymétrique en français. Dans le contexte des réseaux informatiques, cela indique une asymétrie dans le chemin emprunté par les paquets de données lors de leur transfert entre deux points. En d'autres termes, les données suivent des routes différentes en direction et en provenance des points de communication. Cette asymétrie peut être due à divers facteurs tels que des politiques de routage, des différences dans les fournisseurs de services Internet, ou d'autres conditions réseau.

La commande pathping a affiché quatre sauts vers la destination [www.root-me.org](http://www.root-me.org).

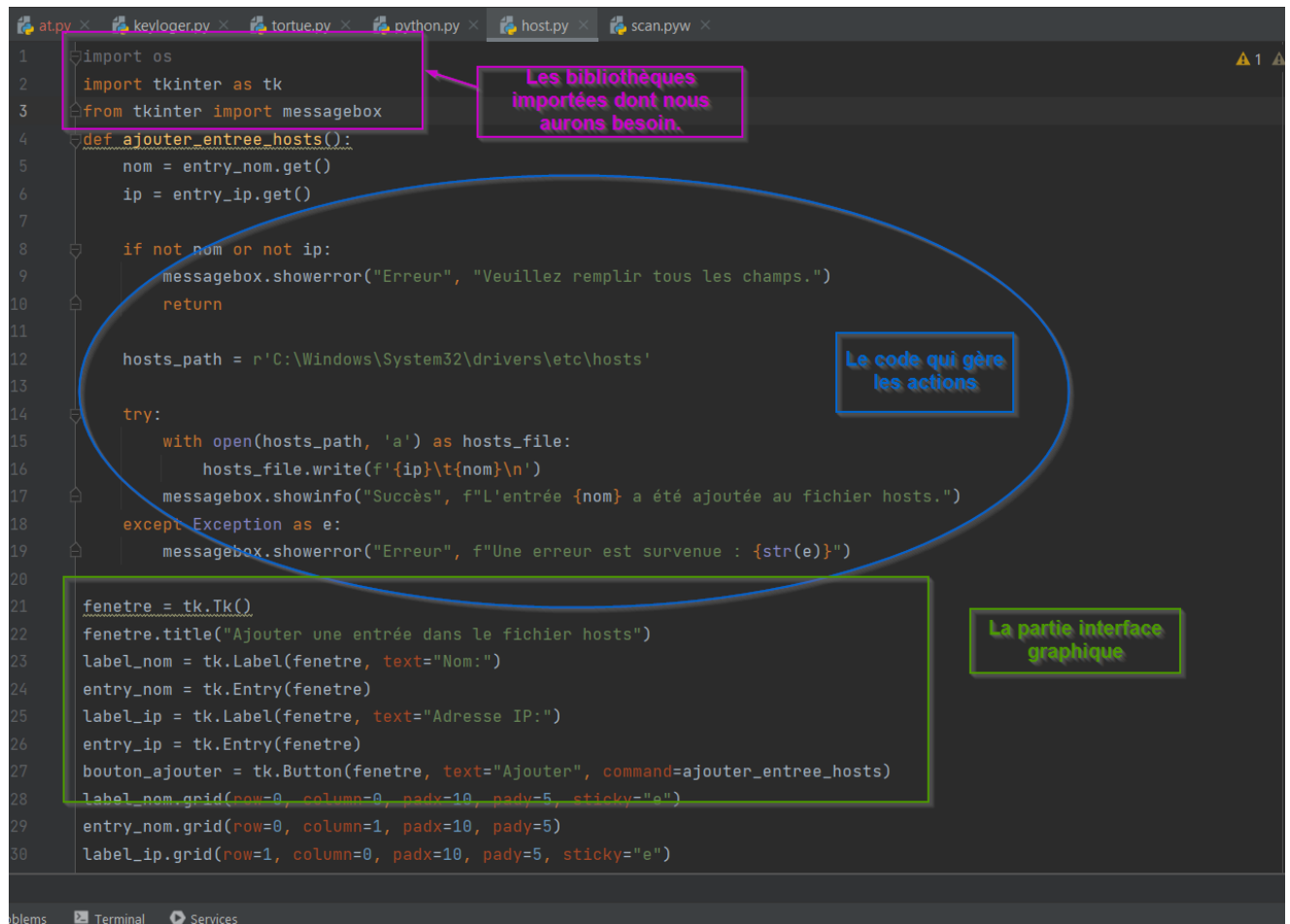
## IX. Fichier host et association réseaux :

Le fichier hosts sous Windows est un fichier texte sans extension qui associe des adresses IP à des noms de domaine. Son rôle principal est de contourner le système de résolution DNS en local, permettant ainsi de spécifier manuellement l'adresse IP à laquelle un nom de domaine particulier doit être résolu.

Ce fichier peut être exploité pour restreindre l'accès à certains sites en redirigeant leur nom de domaine vers une adresse IP locale, comme 127.0.0.1. Cela peut être utilisé, par exemple, pour empêcher un jeune frère de monopoliser la connexion Internet. Il peut également servir à rediriger des noms de domaine vers des adresses IP spécifiques, une technique parfois utilisée par des pirates informatiques, appelée attaque par empoisonnement SEO.

Il est à noter que le fichier hosts a été introduit pour la première fois dans le système d'exploitation BSD en 1983, et Windows a ultérieurement intégré cette fonctionnalité dans ses versions suivantes.

Nous allons explorer les différentes possibilités offertes par ce fichier hosts. Pour ce faire, j'ai créé un script rapide pour simplifier la tâche, surtout dans le cas où un administrateur doit ajouter des dizaines d'entrées dans un fichier hosts. Il peut être essentiel d'avoir un outil permettant de le faire de manière simple et rapide.



The image shows a screenshot of a Python script in a code editor. The script is titled 'host.py' and is used to add entries to the Windows hosts file. The code is annotated with three callouts:

- Les bibliothèques importées dont nous aurons besoin.** (The imported libraries we will need.) - Points to the import statements at lines 1-3.
- Le code qui gère les actions.** (The code that manages the actions.) - Points to the `ajouter_entree_hosts()` function definition and its call at lines 4-19.
- La partie interface graphique.** (The graphical interface part.) - Points to the GUI setup code at lines 21-30.

```
1 import os
2 import tkinter as tk
3 from tkinter import messagebox
4
5 def ajouter_entree_hosts():
6     nom = entry_nom.get()
7     ip = entry_ip.get()
8
9     if not nom or not ip:
10         messagebox.showerror("Erreur", "Veuillez remplir tous les champs.")
11         return
12
13     hosts_path = r'C:\Windows\System32\drivers\etc\hosts'
14
15     try:
16         with open(hosts_path, 'a') as hosts_file:
17             hosts_file.write(f'{ip}\t{nom}\n')
18             messagebox.showinfo("Succès", f"L'entrée {nom} a été ajoutée au fichier hosts.")
19     except Exception as e:
20         messagebox.showerror("Erreur", f"Une erreur est survenue : {str(e)}")
21
22 fenetre = tk.Tk()
23 fenetre.title("Ajouter une entrée dans le fichier hosts")
24 label_nom = tk.Label(fenetre, text="Nom:")
25 entry_nom = tk.Entry(fenetre)
26 label_ip = tk.Label(fenetre, text="Adresse IP:")
27 entry_ip = tk.Entry(fenetre)
28 bouton_ajouter = tk.Button(fenetre, text="Ajouter", command=ajouter_entree_hosts)
29 label_nom.grid(row=0, column=0, padx=10, pady=5, sticky="e")
30 entry_nom.grid(row=0, column=1, padx=10, pady=5)
31 label_ip.grid(row=1, column=0, padx=10, pady=5, sticky="e")
32 entry_ip.grid(row=1, column=1, padx=10, pady=5)
33 bouton_ajouter.grid(row=2, column=1, padx=10, pady=5)
```

Figure 14 Script Python fichier host

L'avantage de ce type de programme, élaboré avec l'aide des bibliothèques tkinter et os, réside dans leur facilité de programmation. Bien que l'interface utilisateur ne soit pas extravagante, elle demeure très pratique. À mon sens, ce sont les meilleures bibliothèques Python pour créer des scripts à usage personnel, particulièrement pour un technicien.

Dans cet exemple, je vais associer l'adresse IP de ma voisine à son prénom. Cela me permettra, par exemple, de la pinguer plus rapidement au sein d'un réseau. Dans le contexte d'une entreprise, où l'on souhaite pinguer un poste ou effectuer des tests à distance, il peut être complexe de mémoriser les adresses IP de chaque poste. Cette approche facilite la tâche d'un technicien qui peut ainsi effectuer des tests sur son collègue Bruno, qui rencontre encore des problèmes à cause du Bluetooth :

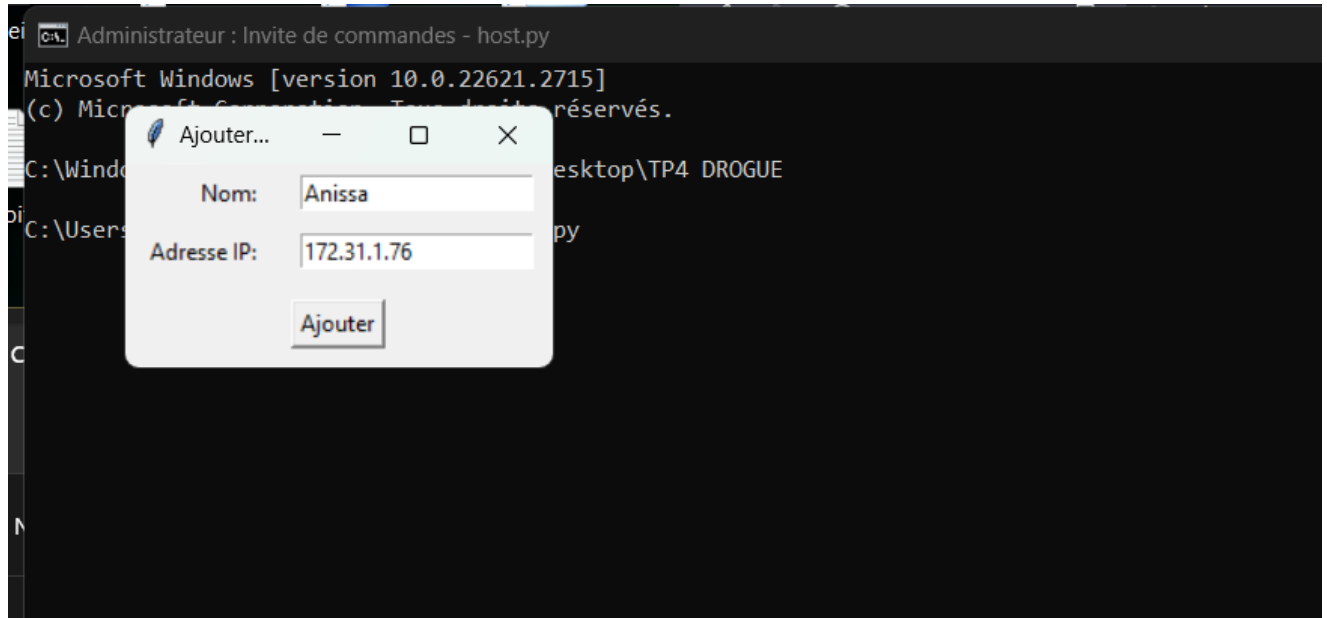


Figure 15 Ajout host

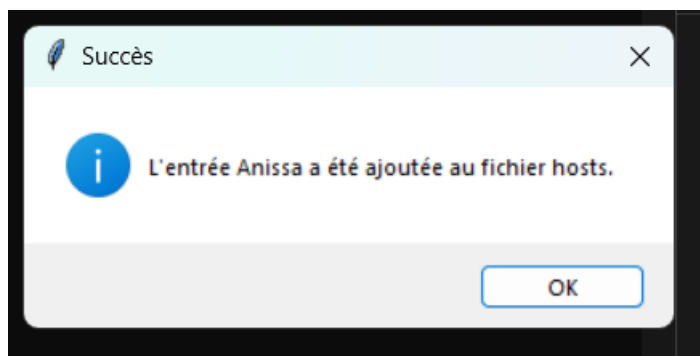
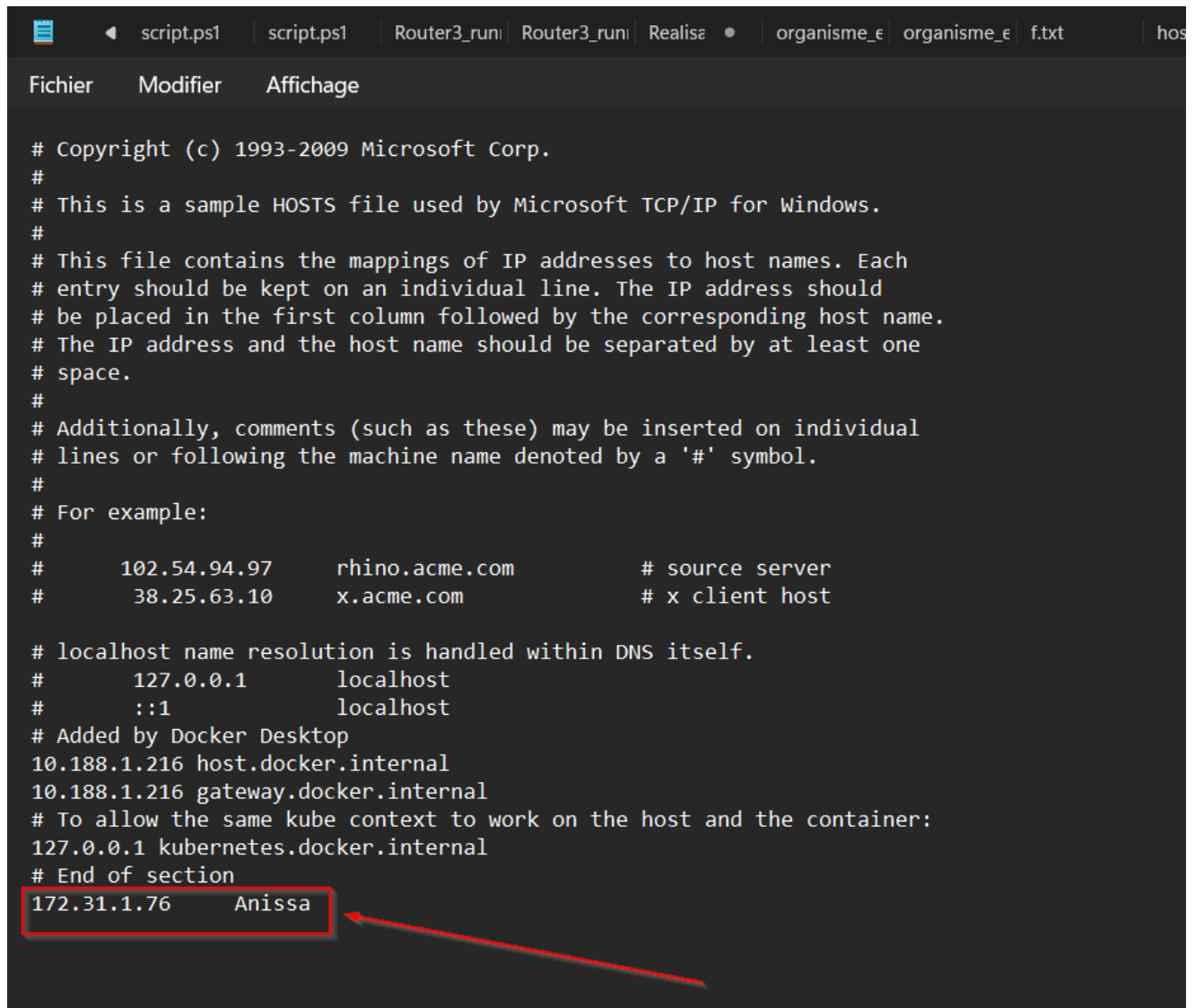


Figure 16



```
# 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
# Added by Docker Desktop
10.188.1.216 host.docker.internal
10.188.1.216 gateway.docker.internal
# To allow the same kube context to work on the host and the container:
127.0.0.1 kubernetes.docker.internal
# End of section
172.31.1.76 Anissa
```

Figure 17 Vérification du fichier host

```
C:\WINDOWS\system32\cmd. x + v
Microsoft Windows [version 10.0.22621.2715]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\eloha>ping Anissa

Envoi d'une requête 'ping' sur Anissa [172.31.1.76] avec 32 octets de données :
Réponse de 172.31.1.76 : octets=32 temps=11 ms TTL=127
Réponse de 172.31.1.76 : octets=32 temps=2 ms TTL=127
Réponse de 172.31.1.76 : octets=32 temps=1 ms TTL=127
Réponse de 172.31.1.76 : octets=32 temps=4 ms TTL=127

Statistiques Ping pour 172.31.1.76:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 11ms, Moyenne = 4ms

C:\Users\eloha>
```

Figure 18 Ping Voisin

```
C:\Users\eloha>nmap -A Anissa
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-15 14:12 Paris, Madrid
NSOCK ERROR [0.3370s] ssl_init_helper(): OpenSSL legacy provider failed to lo

Nmap scan report for Anissa (172.31.1.76)
Host is up (0.017s latency).
Not shown: 997 filtered tcp ports (no-response)
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?
Warning: OSScan results may be unreliable because we could not find at least
Device type: general purpose|specialized
Running (JUST GUESSING): Microsoft Windows XP (89%), AVtech embedded (87%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3
Aggressive OS guesses: Microsoft Windows XP SP3 (89%), AVtech Room Alert 26W
ows XP SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
```

Figure 19 Nmap voisin

J'ai utilisé l'outil nmap pour démontrer que le fichier hosts n'est pas seulement interprété par les commandes de base, mais aussi par les logiciels que nous installons.

**X. Simulation empoisonnement SEO :**

L'empoisonnement par SEO (Search Engine Optimization) est une technique manipulative visant à fausser les résultats des moteurs de recherche. Cela implique généralement la modification de contenu web et de méta-données pour tromper les algorithmes de recherche, augmentant artificiellement le classement d'un site dans les résultats de recherche. L'objectif est d'attirer plus de trafic en exploitant les critères de classement des moteurs de recherche. Cette pratique est contraire aux bonnes pratiques et peut entraîner des sanctions de la part des moteurs de recherche.

Dans notre exemple, je vais illustrer l'utilisation du fichier hosts en associant, par exemple, "google.com" à l'adresse IP de "frameip". Bien sûr, dans des conditions réelles, on peut envisager que le pirate redirigerait vers une fausse page Google pour récupérer nos informations de compte ou imiter une fausse page de banque.

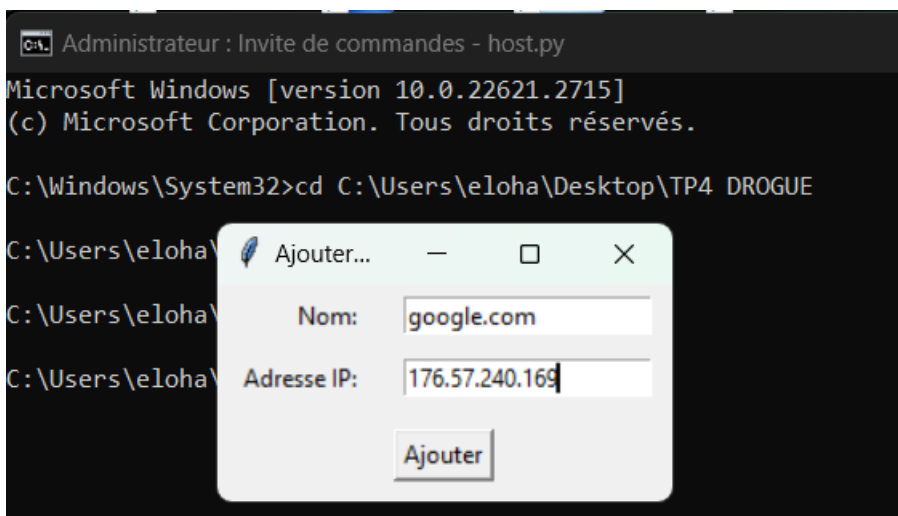


Figure 20 Association google.com

Nos navigateurs modernes détectent facilement que l'adresse IP associée à "google.com" n'est pas normale et signalent une redirection effectuée. Cela s'applique également sur les réseaux publics où l'on vous demande de vous connecter pour accéder à Internet. C'est une mesure de sécurité mise en place par les navigateurs pour tenter de prévenir ce type d'attaque et nous inciter à rester vigilant :



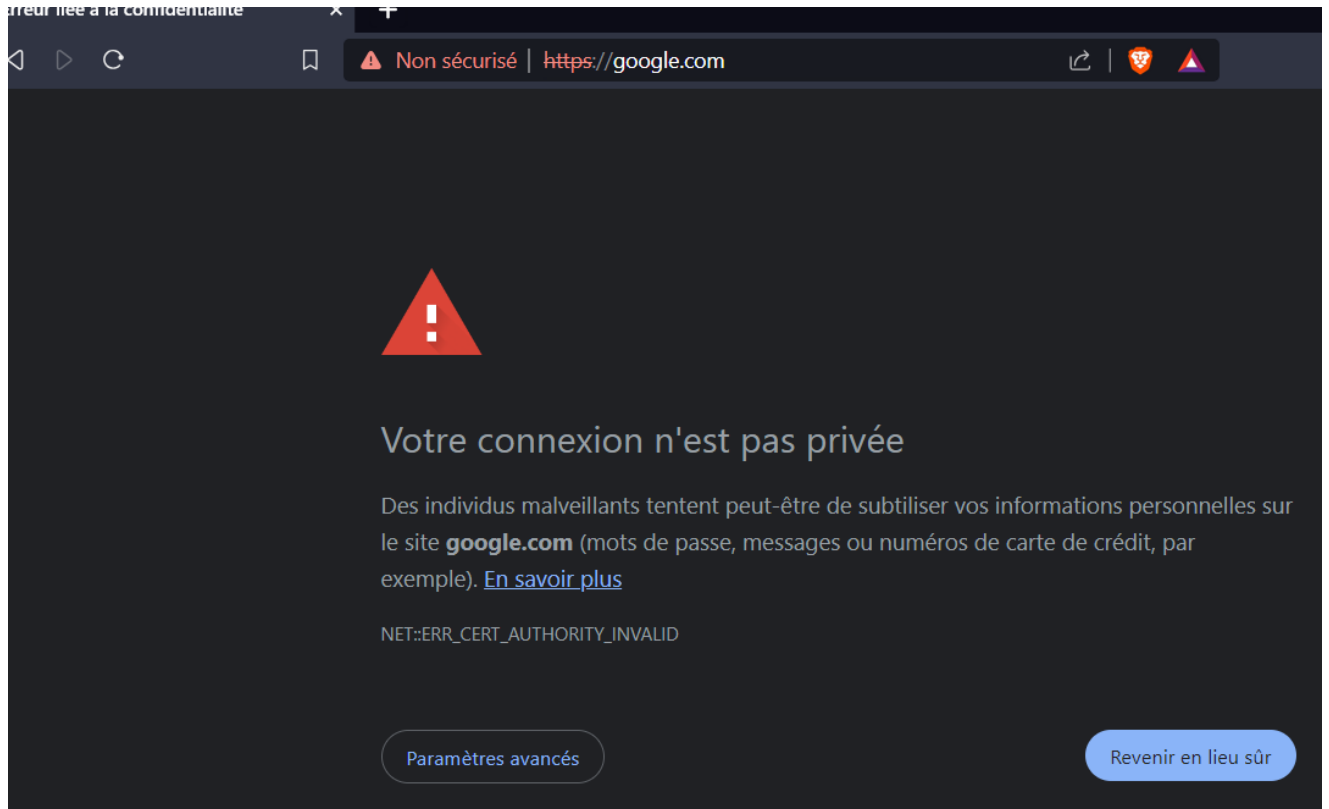
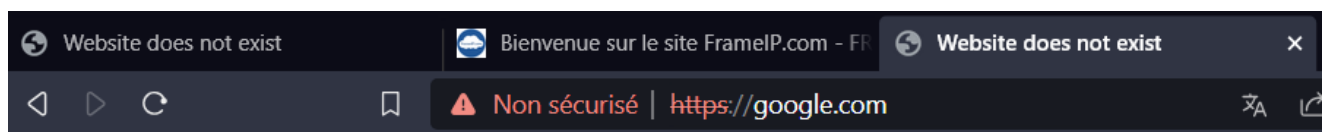


Figure 21 Connexion dangereuse



No valid website found here.

Figure 22 Dns invalide

Le DNS du réseau Sio.local est configuré de manière à privilégier la recherche de réponses en interne avant de chercher sur le réseau extérieur. Cependant, le problème réside dans le fait que l'adresse IP de Frame IP appartient à la même plage d'adresses que le réseau privé du lycée. Par conséquent, dans cette situation, le DNS me redirige vers l'un des appareils internes du réseau Sio.local.

## XI. TTL :

Dans la table DNS, il est possible d'observer que la Durée de Vie (TTL) pour Sublime Text est fixée à 2518 secondes. Les TTL sont utilisés dans le but de limiter la durée pendant laquelle les entrées DNS sont conservées, prévenant ainsi une accumulation indéfinie d'informations qui pourrait encombrer l'ordinateur. Cette fonctionnalité est essentielle car elle permet de retrouver plus rapidement les sites fréquemment visités, évitant ainsi la nécessité de réaliser une requête DNS à chaque accès. En résumé, le TTL contribue à optimiser les performances en régulant la durée de conservation des informations DNS locales.

Si on veut vider cette table on peut avec la commande : `ipconfig /flushdns`

```
www.sublimetext.com
-----
Nom d'enregistrement. : www.sublimetext.com
Type d'enregistrement : 5
Durée de vie . . . . : 2518
Longueur de données . : 8
Section . . . . . : Réponse
Enregistrement CNAME : sublimetext.com

Nom d'enregistrement. : sublimetext.com
Type d'enregistrement : 1
Durée de vie . . . . : 2518
Longueur de données . : 4
Section . . . . . : Réponse
Enregistrement (hôte) : 45.55.41.223
```

On peut constater que le script batch, nommé script1.bat, avait pour objectif d'ajouter une entrée dans le fichier hosts.

## XII. Arp

La commande ARP (Address Resolution Protocol) fonctionne au niveau de la couche 2 du modèle OSI, également connue sous le nom de couche liaison de données. Son rôle principal est de faire correspondre les adresses IP aux adresses physiques (MAC) des dispositifs sur un réseau local. En d'autres termes, ARP facilite la résolution d'adresse au niveau de la couche liaison de données.

```
Microsoft Windows [version 10.0.22621.2715]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\eloha>arp -d

C:\Users\eloha>arp -a

Interface : 192.168.1.199 --- 0x2
Adresse Internet    Adresse physique    Type
224.0.0.22          01-00-5e-00-00-16   statique

Interface : 192.168.56.1 --- 0xd
Adresse Internet    Adresse physique    Type
224.0.0.22          01-00-5e-00-00-16   statique

C:\Users\eloha>arp -s 192.168.1.100 00-aa-11-bb-22-cc
C:\Users\eloha>arp -s 192.168.1.101 11-bb-22-cc-dd-ee
C:\Users\eloha>arp -s 192.168.1.102 22-cc-dd-ee-ff-00
C:\Users\eloha>arp -s 192.168.1.103 33-dd-ee-ff-00-11
C:\Users\eloha>arp -s 192.168.1.104 44-ee-ff-00-11-22

C:\Users\eloha>arp -a

Interface : 192.168.1.199 --- 0x2
Adresse Internet    Adresse physique    Type
192.168.1.1         d8-67-d9-d1-b4-2a   dynamique
192.168.1.100       00-aa-11-bb-22-cc   statique
192.168.1.101       11-bb-22-cc-dd-ee   statique
192.168.1.102       22-cc-dd-ee-ff-00   statique
192.168.1.103       33-dd-ee-ff-00-11   statique
192.168.1.104       44-ee-ff-00-11-22   statique
192.168.1.255       ff-ff-ff-ff-ff-ff   statique
224.0.0.22          01-00-5e-00-00-16   statique
239.255.255.250     01-00-5e-7f-ff-fa   statique

Interface : 192.168.56.1 --- 0xd
Adresse Internet    Adresse physique    Type
192.168.56.255      ff-ff-ff-ff-ff-ff   statique
224.0.0.22          01-00-5e-00-00-16   statique
239.255.255.250     01-00-5e-7f-ff-fa   statique

C:\Users\eloha>
```

On vide le cache ARP.

On affiche la table avec les entrées, en retirant

Ensuite, on ajoute les entrées

Et maintenant, on affiche la nouvelle table.

Le fait d'ajouter des entrées ARP manuellement peut faciliter la communication réseau. Cela peut être intéressant, notamment dans un réseau qui n'évolue pas, où le nombre de postes reste fixe. En désactivant la découverte ARP automatique, on peut empêcher qu'un appareil souhaitant effectuer une attaque « man-in-the-middle » n'ait aucune incidence sur le réseau. En effet, il restera invisible, et aucune communication ne passera par lui, comme s'il était absent.

Ajouter manuellement des entrées ARP facilite la communication, mais cela comporte aussi des risques. Si un pirate diffuse un script malveillant, il pourrait associer ses propres éléments au réseau, se faisant passer pour du matériel légitime. Cela peut conduire à des attaques d'usurpation ARP, mettant en danger la sécurité du réseau. En désactivant la découverte ARP automatique, on perd la protection contre de telles attaques. Il faut donc équilibrer les avantages de la communication facilitée avec les risques potentiels, en mettant en place d'autres mesures de sécurité pour minimiser les menaces.

**g) Réseaux locaux :**

Dans la table ARP, seuls les éléments auxquels nous nous sommes récemment connectés sont répertoriés. De plus, certaines adresses sont supprimées après un certain laps de temps déterminé par une RFC (Request for Comments).

La RFC (Request for Comments) qui définit le temps de vie des entrées ARP (Address Resolution Protocol) est la RFC 826. Elle spécifie le fonctionnement de base de l'ARP et introduit le concept d'un délai de vie (timeout) pour les entrées ARP dans la table. Ce délai de vie détermine pendant combien de temps une entrée ARP reste valide dans la table ARP avant d'être potentiellement supprimée.

```
[Bataillon]
PS C:\Users\eloha> arp -d
PS C:\Users\eloha> arp -a

Interface : 192.168.1.199 --- 0x2
  Adresse Internet    Adresse physique    Type
  192.168.1.1         d8-67-d9-d1-b4-2a   dynamique
  224.0.0.22          01-00-5e-00-00-16   statique

Interface : 192.168.56.1 --- 0xd
  Adresse Internet    Adresse physique    Type
  224.0.0.22          01-00-5e-00-00-16   statique
PS C:\Users\eloha> ping 172.31.1.76

Envoi d'une requête 'Ping' 172.31.1.76 avec 32 octets de données :
Réponse de 172.31.1.76 : octets=32 temps=4 ms TTL=127
Réponse de 172.31.1.76 : octets=32 temps=51 ms TTL=127
Réponse de 172.31.1.76 : octets=32 temps=1 ms TTL=127
Réponse de 172.31.1.76 : octets=32 temps=2 ms TTL=127

Statistiques Ping pour 172.31.1.76:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 51ms, Moyenne = 14ms
PS C:\Users\eloha> arp -a

Interface : 192.168.1.199 --- 0x2
  Adresse Internet    Adresse physique    Type
  192.168.1.1         d8-67-d9-d1-b4-2a   dynamique
  224.0.0.22          01-00-5e-00-00-16   statique

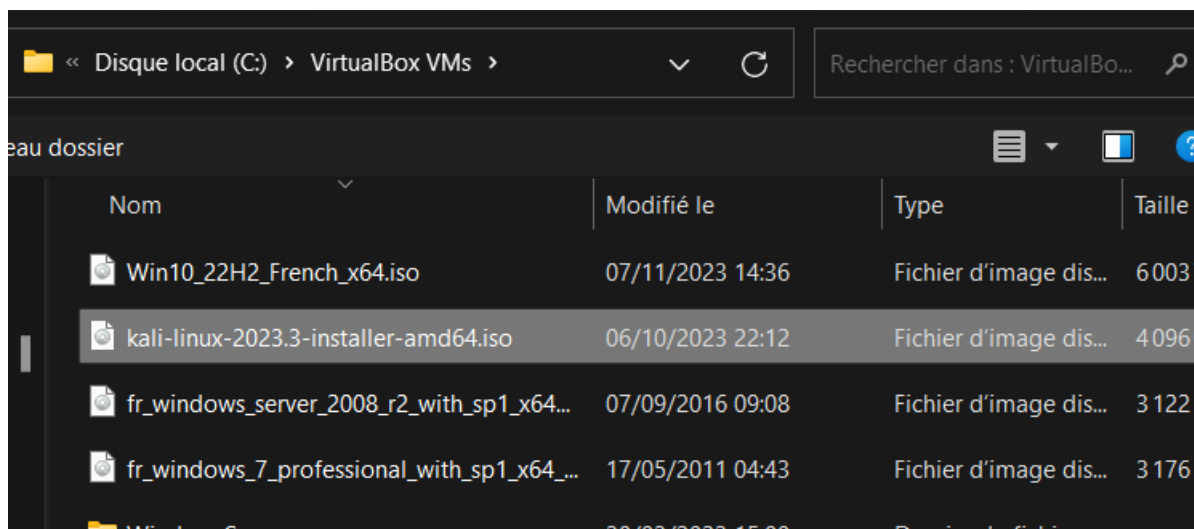
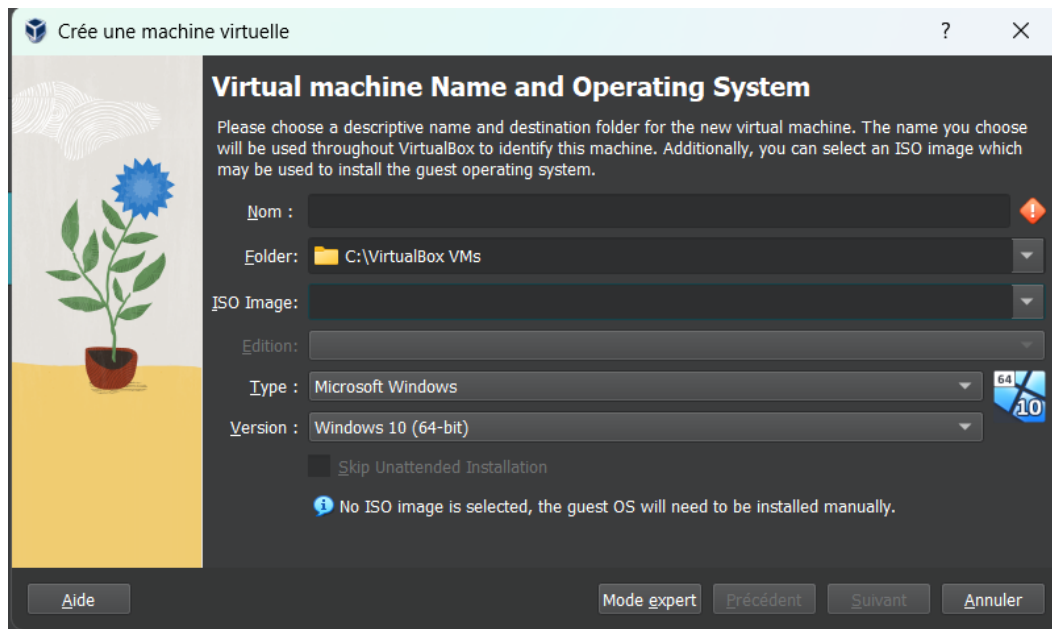
Interface : 192.168.56.1 --- 0xd
  Adresse Internet    Adresse physique    Type
  224.0.0.22          01-00-5e-00-00-16   statique
PS C:\Users\eloha> |
```

**XIII. Machine virtuelle :**

Une machine virtuelle (VM) est un logiciel d'émulation qui simule le fonctionnement d'un ordinateur physique. Elle permet d'exécuter plusieurs systèmes d'exploitation et applications

sur une seule machine physique. Une VM reproduit l'environnement d'un ordinateur, y compris le processeur, la mémoire, le stockage et d'autres périphériques matériels, de manière virtuelle.

Pour cette partie, je montrerai simplement un exemple de création de machine virtuelle, car la mienne est déjà créée et personnalisée avec des outils de pentest avancés :

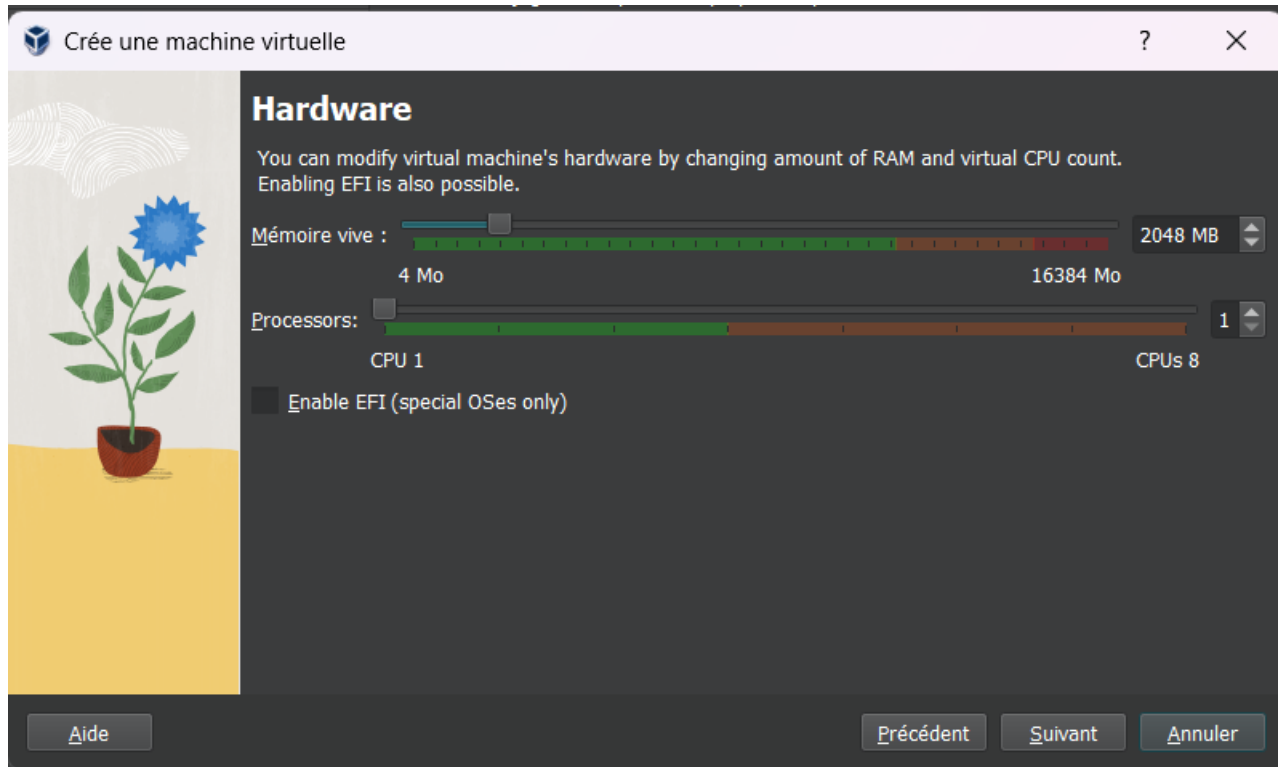


Il est important de choisir un fichier iso pour crée une machine virtuelle personnellement j'ai choisie kali linux :

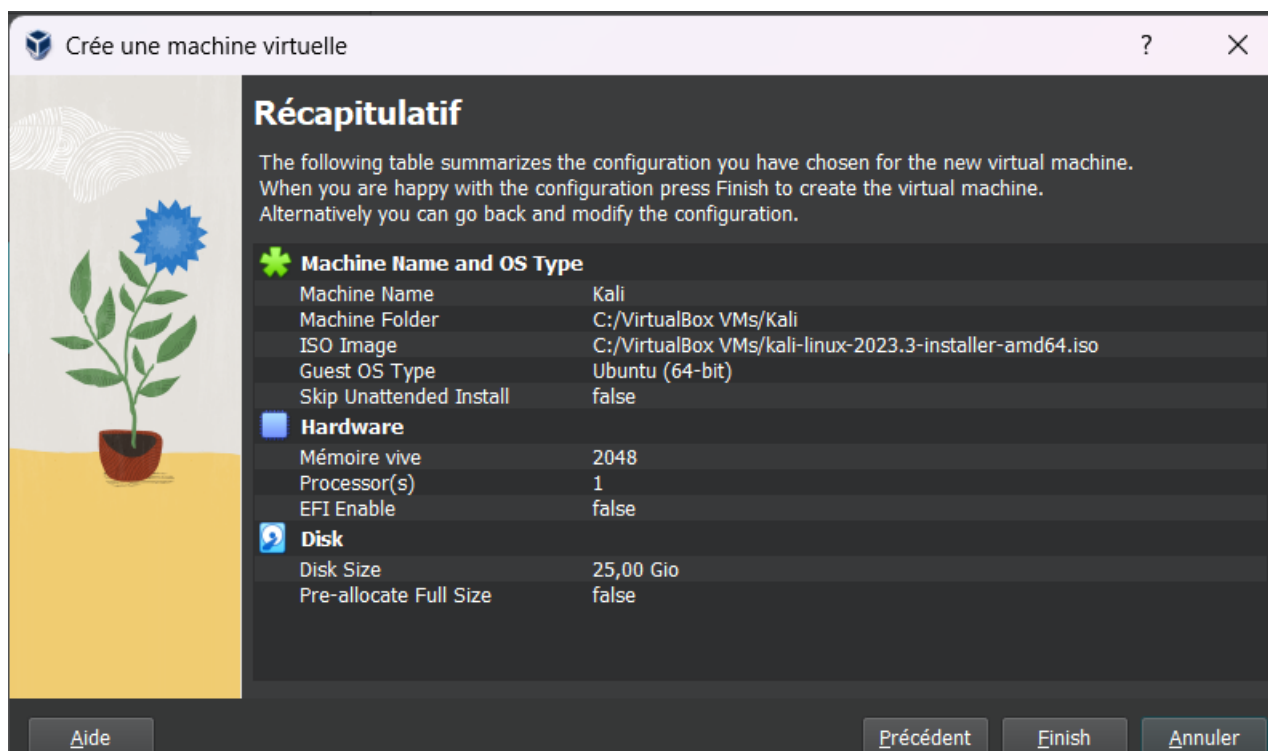
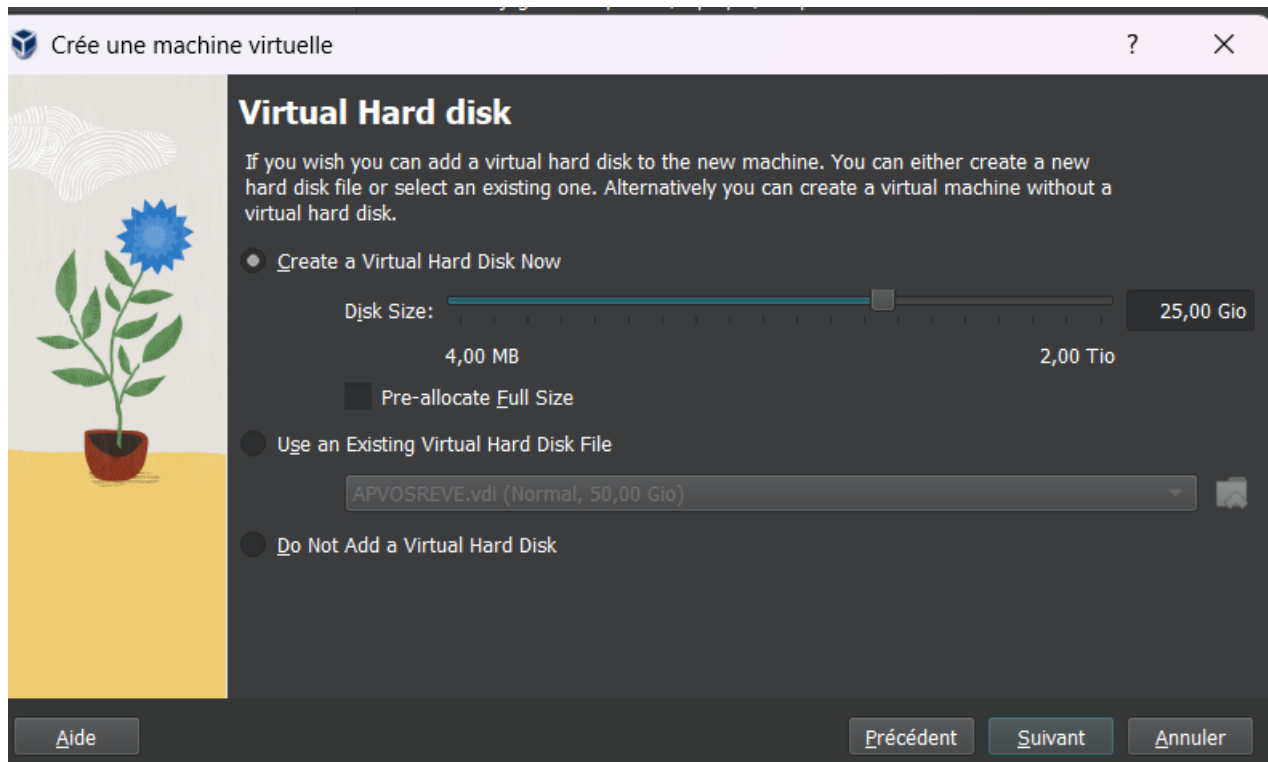
Kali Linux est une distribution Linux dérivée de Debian, développée spécifiquement pour les professionnels de la sécurité informatique, les experts en tests de pénétration (pentesters) et les chercheurs en sécurité. Voici quelques points clés sur son utilisation :

Professionnels de la Sécurité : Kali Linux est largement utilisée par les professionnels de la sécurité informatique, y compris les experts en sécurité, les consultants en sécurité et les administrateurs système. Elle offre une multitude d'outils préinstallés dédiés à la découverte

de vulnérabilités, aux tests d'intrusion, à l'analyse forensique, et à d'autres aspects de la sécurité informatique.

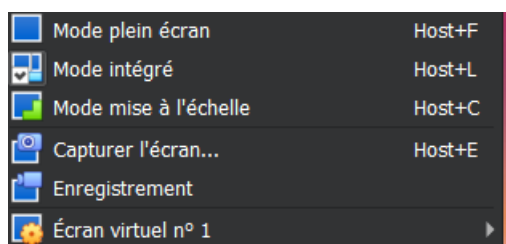


Une machine virtuelle sous Linux nécessite peu de ressources, étant donné que Linux est une distribution très bien optimisée et qu'elle consomme moins de ressources que Windows. Il serait inconcevable de faire fonctionner une machine Windows avec seulement deux giga-octets de RAM. Cependant, une machine Linux fonctionnera de manière plus performante avec 2 giga-octets de RAM qu'une machine Windows avec 8 giga-octets de RAM. C'est l'un des avantages majeurs de Linux.



Linux est largement utilisé en informatique, notamment pour les serveurs, en raison d'un avantage significatif. Par exemple, lors d'une mise à jour, il n'est pas nécessaire de redémarrer le système. En comprenant les pertes qu'une entreprise comme Amazon peut subir si ses services sont inactifs, ne serait-ce que pendant cinq minutes, on saisit facilement l'intérêt de Linux.





Pour mes exemples, j'utiliserai le mode intégré qui combine les avantages de Linux et de Windows, en bénéficiant de la puissance du terminal de Linux avec les outils de Kali Linux sur Windows, tout en profitant de son interface utilisateur.



## h) Outils arp sous linux :

J'ai effectué une première requête en mode administrateur, mais ma commande n'a pas fonctionné en raison des droits d'administrateur.

```
(root@kali) [/home/kali]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::9233:8863:af0a:a256 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:cb:7e:f5 txqueuelen 1000 (Ethernet)
    RX packets 2588 bytes 3550322 (3.3 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1415 bytes 98115 (95.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 20 bytes 1200 (1.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 20 bytes 1200 (1.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(root@kali) [/home/kali]
# arp-scan 10.0.2.15 255.255.255.0
Interface: eth0, type: EN10MB, MAC: 08:00:27:cb:7e:f5, IPv4: 10.0.2.15
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 2 hosts (https://github.com/royhills/arp-scan)
```

J'ai dû exécuter une commande en tant qu'administrateur pour pouvoir utiliser cette fonctionnalité.

```
(root@kali) [/home/kali]
# sudo arp-scan 10.0.2.15/24

Interface: eth0, type: EN10MB, MAC: 08:00:27:cb:7e:f5, IPv4: 10.0.2.15
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
WARNING: host part of 10.0.2.15/24 is non-zero
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
10.0.2.2      52:54:00:12:35:02      (Unknown: locally administered)
10.0.2.3      52:54:00:12:35:03      (Unknown: locally administered)
10.0.2.4      52:54:00:12:35:04      (Unknown: locally administered)

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.874 seconds (136.61 hosts/sec). 3 responded
```

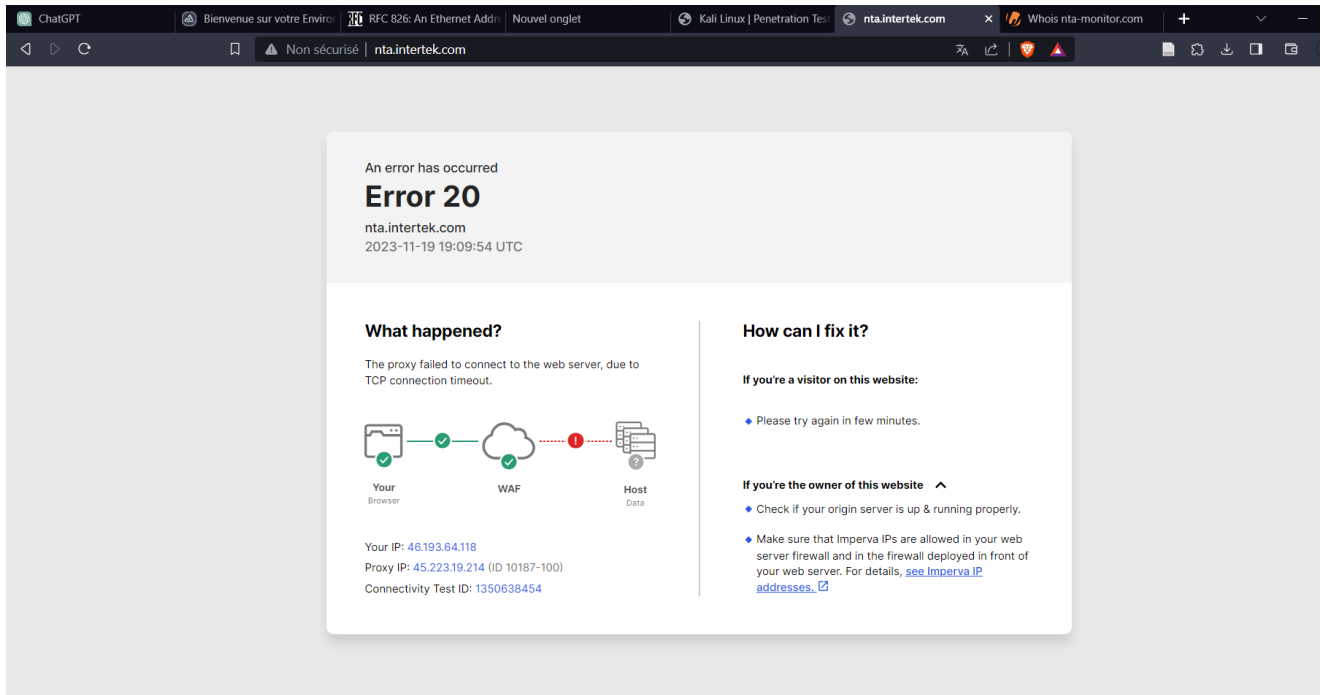
## XIV. Analyse web

Sur la trame que vous nous avez donner on peut trouver un site internet très suspect

```
Interface : eth0, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.9 with 256 hosts (http://www.nta-monitor.com/tools/arp-scan/)
192.168.0.1      20:e5:2a:1b:65:6a      NETGEAR INC..
```

Si l'on essaye de se connecter via le navigateur nous avons une erreur car nous avons rajouté volontairement un www et que le lien original n'en comporte pas.

Ensuite une fois connecté déjà nous sommes en http et impossible de



```
C:\WINDOWS\system32\cmd. x + v
Microsoft Windows [version 10.0.22621.2715]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\eloha>ping http://nta.intertek.com/
La requête Ping n'a pas pu trouver l'hôte http://nta.intertek.com/. Vérifiez le nom et essayez à nouveau.

C:\Users\eloha>ping nta.intertek.com

Envoi d'une requête 'ping' sur 8lnhdz9.x.incapdns.net [45.223.19.214] avec 32 octets de données :
Réponse de 45.223.19.214 : octets=32 temps=12 ms TTL=59
Réponse de 45.223.19.214 : octets=32 temps=13 ms TTL=59
Réponse de 45.223.19.214 : octets=32 temps=12 ms TTL=59
Réponse de 45.223.19.214 : octets=32 temps=13 ms TTL=59

Statistiques Ping pour 45.223.19.214:
  Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
  Minimum = 12ms, Maximum = 13ms, Moyenne = 12ms


C:\Users\eloha>curl -s nta.intertek.com
<html style="height:100%"><head><META NAME="ROBOTS" CONTENT="NOINDEX, NOFOLLOW"><meta name="format-detection" content="telephone=no"><meta name="viewport" content="initial-scale=1.0"><meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1"><script type="text/javascript" src="/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3"></script></head><body style="margin:0px;height:100%"><iframe id="main-iframe" src="/_Incapsula_Resource?CWUDNSAI=4&xinfo=7-68828298-0%20NNNN%20RT%281700421127436%200%29%20q%280%201%20-1%20152%29%20r%28151%20-1%29%20b6%20U18&incident_id=187000700349130935-348056062256681351&edet=20&cinfo=0b0000008e68&rpinfo=0&connaid=1350638454&mth=GET" frameborder=0 width="100%" height="100%" marginheight="0px" marginwidth="0px">Request unsuccessful. Incapsula incident ID: 187000700349130935-348056062256681351</iframe></body></html>
C:\Users\eloha>
```

En effectuant une analyse avec la commande "nmap -A", j'ai remarqué que le site prend beaucoup de temps à se mettre à jour et à communiquer. J'ai l'impression que du code HTML pourrait être présent dans le SSL, ce qui pourrait expliquer une éventuelle erreur et la raison pour laquelle le site ne passe pas en HTTPS. De plus, il semble que le site soit accessible simultanément sur plusieurs ports ouverts, ce qui donne l'impression d'une configuration étrange.

Le site est hébergé par :

```
Network Distance: 7 hops

TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1    2.00 ms   lanspeedtest.wifirst.fr (10.188.0.1)
2    2.00 ms   172.22.4.1
3    ...
4    13.00 ms  172.21.18.246
5    12.00 ms  equinix-paris.core.wifirst.net (195.42.144.142)
6    12.00 ms  imperva_inc.equinix-ix.fr (195.42.145.153)
7    13.00 ms  45.223.19.214
```

 Registrant Contact	
Name:	Blake Barr
Organization:	<b>Intertek Group plc</b>
Street:	25 Savile Row
City:	London
State:	ENG
Postal Code:	W1S 2ES
Country:	GB
Phone:	+44.2073963400
Fax:	+44.2073963480
Email:	<b>donainadmin@intertek.com</b>

Intertek est un prestataire de services leader de l'assurance qualité totale pour les industries à travers le monde. Notre réseau de plus de 1000 laboratoires et bureaux et de plus de 46.000 collaborateurs dans plus de 100 pays, fournit des solutions innovantes et sur mesure d'assurance

## XV. Route :

La table de routage guide les paquets de données à travers le réseau en déterminant le chemin optimal vers leur destination, facilitant la prise de décision pour le routage et permettant la gestion efficace de la connectivité. Cela contribue également à la redondance et à la tolérance de panne dans les réseaux. En cybersécurité des réseaux, la compréhension et la gestion de cette table sont cruciales.

La commande "route" sous Windows est utilisée pour afficher ou modifier la table de routage IP sur un système. La table de routage répertorie les chemins que les paquets de données doivent emprunter pour atteindre des destinations spécifiques. Voici quelques utilisations courantes de la commande "route" :

## IPv4 Table de routage

```
=====
```

Itinéraires actifs :					
Destination réseau	Masque réseau	Adr. passerelle	Adr. interface	Métrique	
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.199	55	
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	
192.168.1.0	255.255.255.0	On-link	192.168.1.199	311	
192.168.1.199	255.255.255.255	On-link	192.168.1.199	311	
192.168.1.255	255.255.255.255	On-link	192.168.1.199	311	
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	192.168.1.199	311	
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	192.168.1.199	311	

```
=====
```

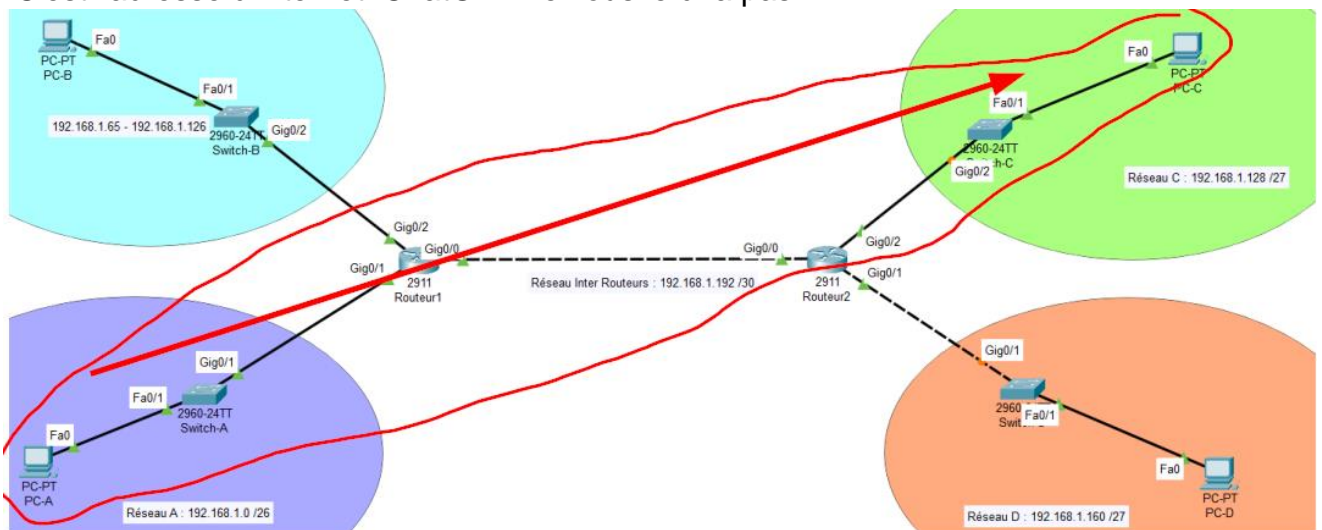
Sous cisco c'est la commande :

```
ip route 192.168.2.0 255.255.255.0 192.168.1.1
```

Nous l'avons utiliser dans l'athelier deux les route ne son utile que pour relier deux ou plusieurs routeur

La première ligne du tableau concerne la route par défaut en IPv4. Elle est représentée par l'adresse de destination "0.0.0.0" avec un masque réseau de "0.0.0.0". Cela signifie que toute destination qui ne correspond à aucune autre route répertoriée dans la table de routage sera dirigée vers la passerelle par défaut dont l'adresse est "192.168.1.1".

"C'est l'adresse d'Internet. ChatGPT ne vous le dira pas."





Comme on peut le voir sur le schéma ci-dessus, une route permet d'indiquer le chemin entre deux réseaux. Il est nécessaire de prévoir un aller et un retour.

10.188.0.0	255.255.0.0	On-link	10.188.1.216	306
------------	-------------	---------	--------------	-----

sur la deuxième ligne de ma table de routage on voit que tout trafic destiné à l'adresse IP dans la plage "10.188.x.x" (masque de sous-réseau 255.255.0.0) sera traité localement sur l'interface réseau avec l'adresse IP "10.188.1.216". Si le trafic est destiné à une adresse IP en dehors de cette plage, alors la passerelle par défaut "10.188.0.1" sera utilisée pour acheminer ce trafic vers d'autres réseaux, y compris Internet.

Donc, toutes nos requêtes passeront par le DHCP (la passerelle par défaut / routeur dans notre cas).

127.0.0.0	255.0.0.0	On-link	127.0.0.1	331
-----------	-----------	---------	-----------	-----

La cinquième ligne correspond à la boucle locale (loopback) de l'adresse IP. Ainsi, toute requête destinée à l'adresse IP dans la plage "127.x.x.x" (masque de sous-réseau 255.0.0.0) sera traitée localement sur l'interface de boucle locale avec l'adresse IP "127.0.0.1"

En IPv6, il n'y a pas d'équivalence directe pour cette ligne car le concept de plage d'adresses de lien local n'est pas directement transposable comme dans IPv4. Cependant, la ligne en IPv6 "fe80::/64 On-link" indique le réseau de lien local, qui est utilisé pour les communications locales sur le même sous-réseau.

## XVI. NetSH

Netsh, abréviation de "Network Shell", est une commande intégrée dans les systèmes d'exploitation Windows, notamment utilisée pour configurer et gérer divers aspects du réseau. Voici quelques-unes des fonctionnalités que permet la commande Netsh :

```
C:\Users\eloha>netsh interface ipv4 show interfaces
```

Idx	Mét	MTU	État	Nom
1	75	4294967295	connected	Loopback Pseudo-Interface 1
2	25	1500	disconnected	Wi-Fi
8	25	1500	connected	Ethernet
16	25	1500	disconnected	Connexion au réseau local* 1
10	25	1500	disconnected	Connexion au réseau local* 2
13	25	1500	connected	Ethernet 3

En fonction de ces informations, vous pouvez voir l'état de chaque interface, qu'elles soient connectées ou déconnectées, leur type (filaire ou sans fil), et d'autres détails tels que la métrique et la taille maximale des paquets.

On peut afficher toute l'interface avec cette commande d'après Chat Gpt, mais j'ai plus d'interface avec le premier résultat.

```
C:\Users\eloha>netsh interface show interface
```

État admin	État	Type	Nom de l'interface
Activé	Connecté	Dédié	Ethernet 3
Activé	Déconnecté	Dédié	Wi-Fi
Activé	Connecté	Dédié	Ethernet
Activé	Déconnecté	Dédié	Connexion au réseau local* 2

Cette commande, `netsh interface ipv4 show neighbors`, permet, comme son nom "Neighbors" l'indique, d'afficher les interfaces des voisins. Les résultats de la commande sont présentés de manière concise, et vous pouvez trouver des détails supplémentaires dans les documents textes en annexe.

```
PS C:\Users\eloha> netsh interface ipv4 show neighbors
```

Interface 1 : Loopback Pseudo-Interface 1

Adresse Internet	Adresse physique	Type
224.0.0.22		Permanent
226.178.217.5		Permanent
239.255.255.255		Permanent

Interface 2 : Wi-Fi

Adresse Internet	Adresse physique	Type
192.168.1.1	d8-67-d9-d1-b4-2a	Caducue
192.168.1.199	00-00-00-00-00-00	Inaccessible
192.168.1.255	ff-ff-ff-ff-ff-ff	Permanent
224.0.0.22	01-00-5e-00-00-16	Permanent
224.0.0.251	01-00-5e-00-00-fb	Permanent
224.0.0.252	01-00-5e-00-00-fc	Permanent
239.255.255.255	01-00-5e-7f-ff-fa	Permanent
255.255.255.255	ff-ff-ff-ff-ff-ff	Permanent

Interface 8 : Ethernet

Adresse Internet	Adresse physique	Type
169.254.255.255	00-00-00-00-00-00	Inaccessible
172.31.1.4	00-19-99-b7-bf-27	Caducue
172.31.1.6	00-50-56-b7-c9-34	Caducue
172.31.1.7	00-50-56-b7-14-20	Caducue
172.31.1.9	00-50-56-bc-3a-7c	Caducue
172.31.1.31	00-11-32-90-09-25	Caducue
172.31.1.56	00-00-00-00-00-00	Inaccessible
172.31.1.61	00-50-56-ab-e5-08	Caducue
172.31.1.68	24-be-05-18-1d-1c	Caducue
172.31.1.74	00-00-00-00-00-00	Inaccessible
172.31.1.253	00-00-00-00-00-00	Inaccessible
172.31.1.254	00-0c-29-b8-25-53	Joignable
172.31.1.255	ff-ff-ff-ff-ff-ff	Permanent
224.0.0.22	01-00-5e-00-00-16	Permanent
224.0.0.251	01-00-5e-00-00-fb	Permanent
224.0.0.252	01-00-5e-00-00-fc	Permanent
239.255.182.18	01-00-5e-7f-ff-fa	Permanent
239.255.255.255	ff-ff-ff-ff-ff-ff	Permanent

Interface 16 : Connexion au réseau local\* 1

Adresse Internet	Adresse physique	Type
224.0.0.22	01-00-5e-00-00-16	Permanent
226.178.217.5	01-00-5e-32-d9-05	Permanent

Interface 18 : Connexion au réseau local\* 2

Adresse Internet	Adresse physique	Type
224.0.0.22	01-00-5e-00-00-16	Permanent

Interface 13 : Ethernet 3

Adresse Internet	Adresse physique	Type
192.168.56.255	ff-ff-ff-ff-ff-ff	Permanent
224.0.0.22	01-00-5e-00-00-16	Permanent
224.0.0.251	01-00-5e-00-00-fb	Permanent
224.0.0.252	01-00-5e-00-00-fc	Permanent
226.178.217.5	01-00-5e-32-d9-05	Permanent
239.255.255.255	01-00-5e-7f-ff-fa	Permanent

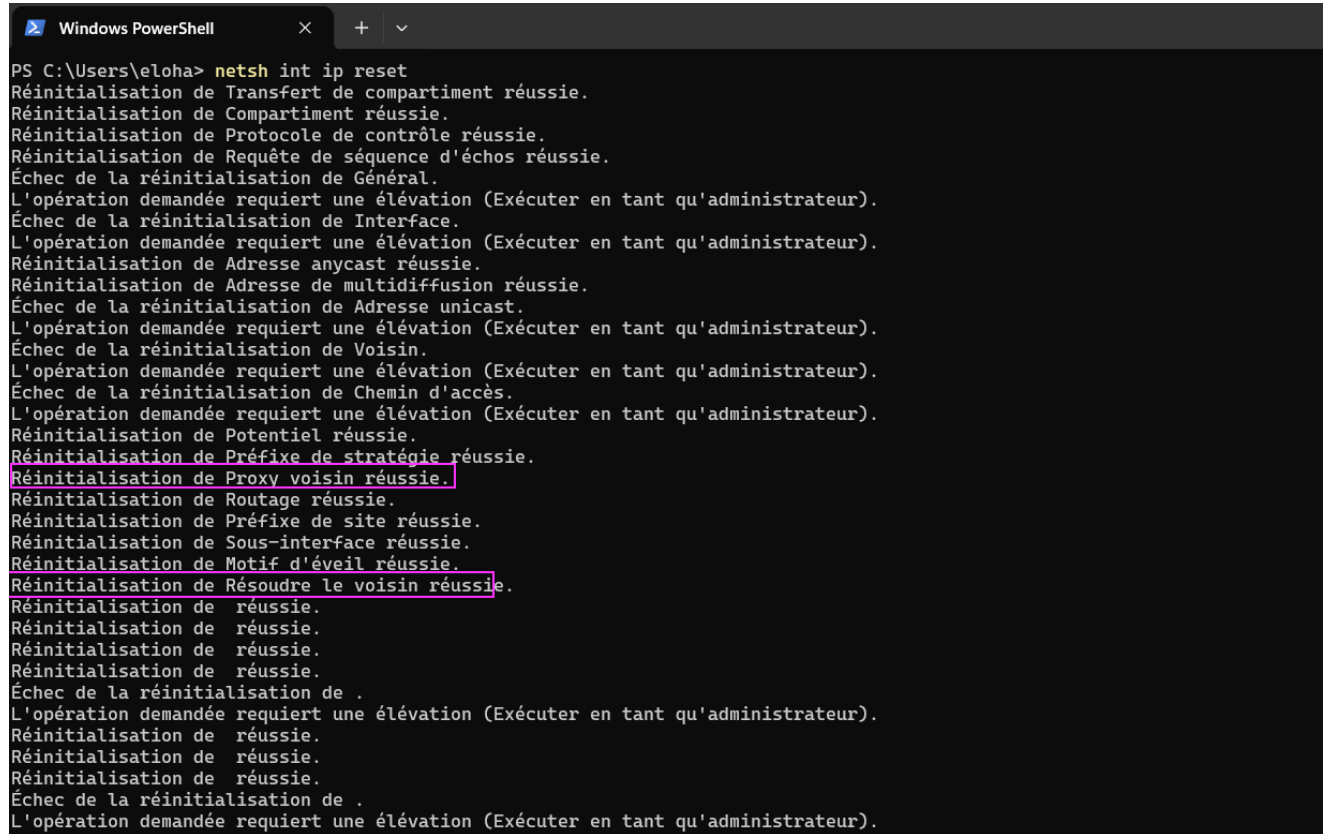
```
PS C:\Users\eloha>
```

Globalement, on pourrait dire que cette commande affiche la table ARP des voisins.

### i) Réinitialisation de la pile IP

netsh int ip reset

Parfois, votre ordinateur peut rencontrer des difficultés de connexion en raison d'une pile IP défectueuse. Dans de tels cas, il est essentiel de pouvoir réinitialiser la pile IP.



```
PS C:\Users\eloha> netsh int 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.
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).
```

Dans notre situation, il est observé que la réinitialisation de la pile IP entraîne également la réinitialisation des piles **voisines**.

### j) Commande d'analyse

Si l'on cherche une commande avancée fournissant des informations détaillées et complètes, la commande "systeminfo" s'impose. Elle affiche de manière exhaustive les détails de tous les composants, y compris des informations sur le compte Windows et un résumé des informations réseau.



```
C:\Users\eloha>systeminfo

Nom de l'hôte: N15I516BK512
Nom du système d'exploitation: Microsoft Windows 11 Famille
Version du système: 10.0.22621 N/A build 22621
Fabricant du système d'exploitation: Microsoft Corporation
Configuration du système d'exploitation: Station de travail autonome
Type de build du système d'exploitation: Multiprocessor Free
Propriétaire enregistré: eloham.caron@gmail.com
Organisation enregistrée: N/A
Identificateur de produit: 00325-85350-38752-AAOEM
Date d'installation originale: 09/01/2023, 01:54:09
Heure de démarrage du système: 22/11/2023, 13:28:04
Fabricant du système: THOMSON
Modèle du système: N15I5
Type du système: x64-based PC
Processeur(s): 1 processeur(s) installé(s).
[01] : Intel64 Family 6 Model 142 Stepping 10 GenuineIntel ~2304 MHz
Version du BIOS: American Megatrends Inc. CN1GFV604, 21/06/2022
Répertoire Windows: C:\WINDOWS
Répertoire système: C:\WINDOWS\system32
Périphérique d'amorçage: \Device\HarddiskVolume1
Option régionale du système: fr;Français (France)
Paramètres régionaux d'entrée: fr;Français (France)
Fuseau horaire: (UTC+01:00) Bruxelles, Copenhagen, Madrid, Paris
Mémoire physique totale: 16 277 Mo
Mémoire physique disponible: 11 510 Mo
Mémoire virtuelle : taille maximale: 17 301 Mo
Mémoire virtuelle : disponible: 12 745 Mo
Mémoire virtuelle : en cours d'utilisation: 4 556 Mo
Emplacements des fichiers d'échange: C:\pagefile.sys
Domaine: WORKGROUP
Serveur d'ouverture de session: \\N15I516BK512
Correctif(s): 4 Corrections installées.
[01]: KB5032007
[02]: KB5012170
```

Cependant, je pense que cette commande serait plus complète si nous utilisions "**netstat - a**", une commande entièrement axée sur le réseau. Elle se complète parfaitement avec la commande "**systeminfo**".

```
C:\Users\eloha>netstat -a
```

#### Connexions actives

Proto	Adresse locale	Adresse distante	État
TCP	0.0.0.0:135	N15I516BK512:0	LISTENING
TCP	0.0.0.0:445	N15I516BK512:0	LISTENING
TCP	0.0.0.0:5040	N15I516BK512:0	LISTENING
TCP	0.0.0.0:5357	N15I516BK512:0	LISTENING
TCP	0.0.0.0:5432	N15I516BK512:0	LISTENING
TCP	0.0.0.0:7070	N15I516BK512:0	LISTENING
TCP	0.0.0.0:49664	N15I516BK512:0	LISTENING
TCP	0.0.0.0:49665	N15I516BK512:0	LISTENING
TCP	0.0.0.0:49666	N15I516BK512:0	LISTENING
TCP	0.0.0.0:49667	N15I516BK512:0	LISTENING
TCP	0.0.0.0:49669	N15I516BK512:0	LISTENING
TCP	0.0.0.0:49675	N15I516BK512:0	LISTENING
TCP	127.0.0.1:5939	N15I516BK512:0	LISTENING
TCP	127.0.0.1:6463	N15I516BK512:0	LISTENING
TCP	127.0.0.1:20000	N15I516BK512:0	LISTENING
TCP	127.0.0.1:20000	kubernetes:49706	ESTABLISHED
TCP	127.0.0.1:20000	kubernetes:49731	ESTABLISHED
TCP	127.0.0.1:21320	N15I516BK512:0	LISTENING
TCP	127.0.0.1:21321	N15I516BK512:0	LISTENING
TCP	127.0.0.1:21322	N15I516BK512:0	LISTENING

La commande netstat -a affiche les connexions réseau actives et les ports en écoute sur un système. Voici une explication détaillée de chaque partie de la commande :

#### k) Analyse des communications :

L'ordinateur en question a plusieurs connexions actives, avec différentes adresses IP distantes. Voici quelques exemples de connexions établies :

- Connexion avec l'adresse IP distante 51.178.91.234 sur le port 6568.
- Connexion avec l'adresse IP distante 40.74.219.49 sur le port 443.
- Connexion avec l'adresse IP distante 20.199.120.85 sur le port 443.
- Connexion avec l'adresse IP distante 52.42.216.19 sur le port 443.
- Connexion avec l'adresse IP distante 64.91.226.82 sur le port 443.

Diverses connexions en local avec l'adresse IP 127.0.0.1 sur différents ports.

La liste complète des connexions actives montre avec qui l'ordinateur est en communication à un moment donné.

Comme on peut le constater ci-dessous, tous ces ports sont ouverts, certains étant associés à des services, d'autres non. Avoir tous ces ports et services ouverts représente une faille de sécurité considérable. C'est catastrophique d'avoir autant de services et de ports ouverts, à moins d'être sur un réseau expertement configuré. Cependant, en observant cette configuration, j'ai l'impression que la personne ne surveille pas les ports ouverts de son ordinateur, ce qui est particulièrement préoccupant.

- Port 135 : Protocole RPC (Remote Procedure Call), souvent utilisé par Microsoft Windows pour divers services.
- Port 139 : NetBIOS Session Service, utilisé pour le partage de fichiers et d'imprimantes sur les réseaux Windows.
- Port 808 : Protocole HTTP alternatif, parfois utilisé pour des applications personnalisées.
- Port 1033 : Utilisé pour divers services, peut être associé à des applications spécifiques.
- Port 1035 : Protocole de résolution de noms de domaine (DNS).
- Port 1047 : Communication sécurisée sur le port HTTPS (443) vers une adresse distante.
- Port 1072 : Communication sécurisée sur le port HTTPS (443) vers une autre adresse distante.
- Ports 1080-1094 : Ils sont utilisés pour divers services, parfois associés à des protocoles tels que SOCKS.
- Port 1149 : Communication sécurisée sur le port HTTPS (443) vers une adresse distante.
- Ports 1157-1164 : Utilisés pour divers services, parfois associés à des protocoles de communication spécifiques.
- Port 1185 : Communication sur le port HTTPS (443) vers une adresse distante.
- Ports 1194, 3275, 5040, 5354, 7070 : Utilisés pour divers services, nécessiterait une analyse plus approfondie pour des détails spécifiques.
- Ports 8384, 8386, 22000, 22001 : Souvent utilisés par des applications liées à la gestion et la synchronisation de fichiers (par exemple, Syncthing).

**XVII.** Netstat :

La commande `netstat` affiche des informations sur les connexions réseau, les ports, les tables de routage et d'autres statistiques réseau. Les options utilisées, comme `-an`, spécifient le format de sortie et la sélection des informations à afficher, telles que les connexions TCP et UDP en écoute.

```
Windows PowerShell
PS C:\Users\eloha> netstat -an | Select-String "TCP" | Select-String "LISTEN"

TCP    0.0.0.0:135           0.0.0.0:0           LISTENING
TCP    0.0.0.0:445         0.0.0.0:0           LISTENING
TCP    0.0.0.0:5040        0.0.0.0:0           LISTENING
TCP    0.0.0.0:5357        0.0.0.0:0           LISTENING
TCP    0.0.0.0:5432        0.0.0.0:0           LISTENING
TCP    0.0.0.0:7070        0.0.0.0:0           LISTENING
TCP    0.0.0.0:49664       0.0.0.0:0           LISTENING
TCP    0.0.0.0:49665       0.0.0.0:0           LISTENING
TCP    0.0.0.0:49666       0.0.0.0:0           LISTENING
TCP    0.0.0.0:49667       0.0.0.0:0           LISTENING
TCP    0.0.0.0:49668       0.0.0.0:0           LISTENING
TCP    0.0.0.0:49670       0.0.0.0:0           LISTENING
TCP    127.0.0.1:5939      0.0.0.0:0           LISTENING
TCP    127.0.0.1:20000     0.0.0.0:0           LISTENING
TCP    127.0.0.1:21320     0.0.0.0:0           LISTENING
TCP    127.0.0.1:21321     0.0.0.0:0           LISTENING
TCP    127.0.0.1:21322     0.0.0.0:0           LISTENING
TCP    127.0.0.1:21323     0.0.0.0:0           LISTENING
TCP    127.0.0.1:27015     0.0.0.0:0           LISTENING
TCP    172.31.1.54:139     0.0.0.0:0           LISTENING
TCP    192.168.56.1:139    0.0.0.0:0           LISTENING
```

```
PS C:\Users\eloha> netstat -an | Select-String "UDP"

UDP    0.0.0.0:67          *:*
UDP    0.0.0.0:123         *:*
UDP    0.0.0.0:500         *:*
UDP    0.0.0.0:3702        *:*
UDP    0.0.0.0:3702        *:*
UDP    0.0.0.0:4500        *:*
UDP    0.0.0.0:5050        *:*
UDP    0.0.0.0:5353        *:*
UDP    0.0.0.0:5355        *:*
UDP    0.0.0.0:21328       *:*
UDP    0.0.0.0:49429       *:*
UDP    0.0.0.0:50001       *:*
UDP    0.0.0.0:51605       *:*
UDP    0.0.0.0:51633       172.64.150.28:443
UDP    0.0.0.0:55983       *:*
UDP    0.0.0.0:55984       *:*
UDP    0.0.0.0:56216       172.217.20.170:443
UDP    0.0.0.0:63949       *:*
UDP    0.0.0.0:64057       34.120.214.181:443
```

l) Pour obtenir les statistiques d'utilisation d'Ethernet

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


```

	Reçus	Émis
Octets	129914576	21580992
Paquets monodiffusion	140248	82368
Paquets non monodiffusion	0	3944
Rejets	0	0
Erreurs	0	0
Protocoles inconnus	0	

```
C:\Users\eloha>
```

Avec la commande netstat -s, vous pouvez consulter les statistiques spécifiques IPv4 et IPv6 pour les protocoles tels que ICMP, TCP, etc., sur différentes interfaces.

```
C:\Users\eloha>netstat -s
```

#### Statistiques IPv4

Paquets Reçus	= 18650
Erreurs d'en-tête reçues	= 0
Erreurs d'adresse reçues	= 0
Datagrammes transférés	= 0
Protocoles inconnus reçus	= 0
Paquets reçus rejetés	= 75
Paquets reçus délivrés	= 19387
Requêtes en sortie	= 12587
Routages rejetés	= 0
Paquets en sortie rejetés	= 0
Paquet en sortie non routés	= 3
Réassemblage requis	= 306
Réassemblage réussi	= 51
Défaillances de réassemblage	= 0
Fragmentations de datagrammes réussies	= 3
Fragmentations de datagrammes défaillantes	= 0
Fragments Créés	= 12

#### Statistiques IPv6

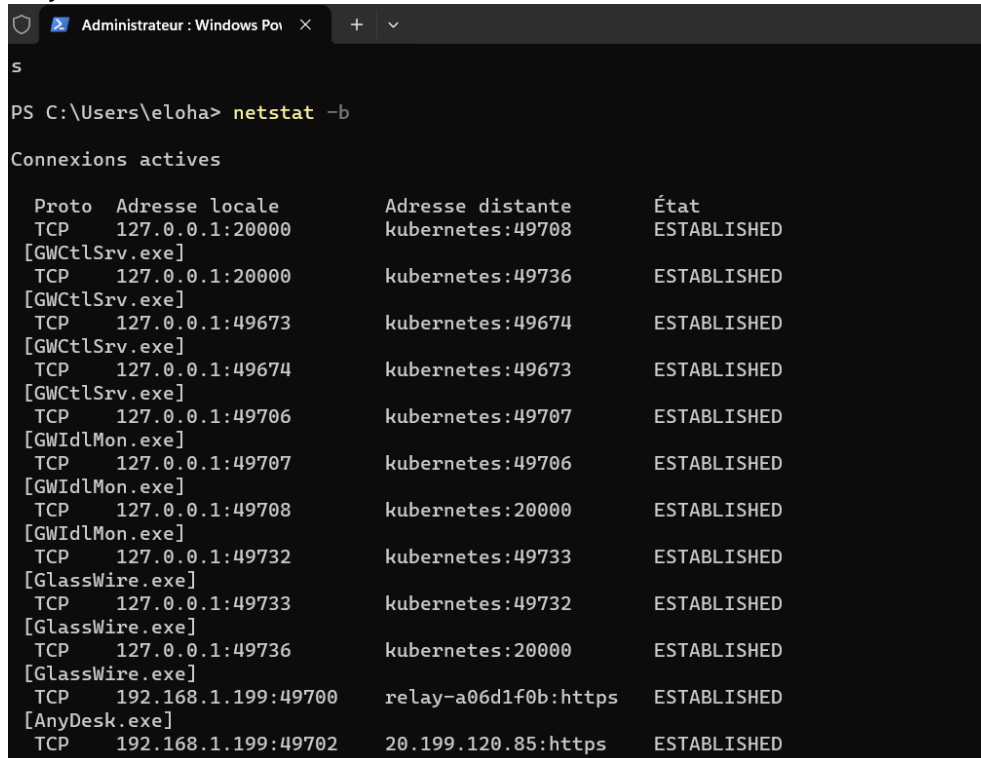
Paquets Reçus	= 0
Erreurs d'en-tête reçues	= 0
Erreurs d'adresse reçues	= 0
Datagrammes transférés	= 0
Protocoles inconnus reçus	= 0
Paquets reçus rejetés	= 0
Paquets reçus délivrés	= 308
Requêtes en sortie	= 516
Routages rejetés	= 0
Paquets en sortie rejetés	= 0
Paquet en sortie non routés	= 0
Réassemblage 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	0	12
Erreurs	0	0
Destination inaccessible	0	12
Temps dépassé	0	0
Problèmes de paramètres	0	0
La source s'éteint	0	0
Redirections	0	0
Réponses échos	0	0
Echos	0	0
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

**m) Les noms des fichiers exécutables impliqués dans la création de la connexion**

Le nom des fichiers est indiqué au début, par exemple : GWctlSrv.exe, GlassWire.exe, AnyDesk.exe, svchost.exe, WINWORD.EXE.



```
PS C:\Users\eloha> netstat -b

Connexions actives

Proto  Adresse locale      Adresse distante     État
-----
TCP    127.0.0.1:20000      kubernetes:49708     ESTABLISHED
[GWctlSrv.exe]
TCP    127.0.0.1:20000      kubernetes:49736     ESTABLISHED
[GWctlSrv.exe]
TCP    127.0.0.1:49673      kubernetes:49674     ESTABLISHED
[GWctlSrv.exe]
TCP    127.0.0.1:49674      kubernetes:49673     ESTABLISHED
[GWctlSrv.exe]
TCP    127.0.0.1:49706      kubernetes:49707     ESTABLISHED
[GWIdlMon.exe]
TCP    127.0.0.1:49707      kubernetes:49706     ESTABLISHED
[GWIdlMon.exe]
TCP    127.0.0.1:49708      kubernetes:20000     ESTABLISHED
[GWIdlMon.exe]
TCP    127.0.0.1:49732      kubernetes:49733     ESTABLISHED
[GlassWire.exe]
TCP    127.0.0.1:49733      kubernetes:49732     ESTABLISHED
[GlassWire.exe]
TCP    127.0.0.1:49736      kubernetes:20000     ESTABLISHED
[GlassWire.exe]
TCP    192.168.1.199:49700  relay-a06d1f0b:https ESTABLISHED
[AnyDesk.exe]
TCP    192.168.1.199:49702  20.199.120.85:https  ESTABLISHED
```

Le numéro du processus associé à chaque connexion

```
C:\WINDOWS\system32\cmd. X + v
Microsoft Windows [version 10.0.22621.2715]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\eloha>netstat -o

Connexions actives
```

Proto	Adresse locale	Adresse distante	État	
TCP	127.0.0.1:20000	kubernetes:49708	ESTABLISHED	4912
TCP	127.0.0.1:20000	kubernetes:49736	ESTABLISHED	4912
TCP	127.0.0.1:49673	kubernetes:49674	ESTABLISHED	4912
TCP	127.0.0.1:49674	kubernetes:49673	ESTABLISHED	4912
TCP	127.0.0.1:49706	kubernetes:49707	ESTABLISHED	9772
TCP	127.0.0.1:49707	kubernetes:49706	ESTABLISHED	9772
TCP	127.0.0.1:49708	kubernetes:20000	ESTABLISHED	9772
TCP	127.0.0.1:49732	kubernetes:49733	ESTABLISHED	9060
TCP	127.0.0.1:49733	kubernetes:49732	ESTABLISHED	9060
TCP	127.0.0.1:49736	kubernetes:20000	ESTABLISHED	9060
TCP	192.168.1.199:49700	relay-a06d1f0b:https	ESTABLISHED	4240
TCP	192.168.1.199:49702	20.199.120.85:https	ESTABLISHED	4136
TCP	192.168.1.199:50336	162.159.128.233:https	ESTABLISHED	13544
TCP	192.168.1.199:50337	162.159.130.234:https	ESTABLISHED	13544
TCP	192.168.1.199:50339	162.159.137.232:https	ESTABLISHED	13544
TCP	192.168.1.199:50340	25:https	ESTABLISHED	13544
TCP	192.168.1.199:50341	162.159.130.233:https	ESTABLISHED	13544
TCP	192.168.1.199:50342	192:https	ESTABLISHED	13544
TCP	192.168.1.199:50344	162.159.130.232:https	ESTABLISHED	13544
TCP	192.168.1.199:50350	162.159.138.234:https	ESTABLISHED	13544
TCP	192.168.1.199:50359	server-18-155-129-28:https	ESTABLISHED	1372
TCP	192.168.1.199:50362	server-13-249-9-26:https	ESTABLISHED	1372

Un numéro est associé à "plusieurs" connexions, étant donné que c'est la même connexion. On utilise des ports et des services différents, c'est pourquoi certaines requêtes ont le même numéro.



## **XVIII. Etape Bonus NMAP :**

Nmap, abréviation de "Network Mapper", est un outil de scanner de réseau open source utilisé pour découvrir des hôtes et des services sur un réseau, ainsi que pour créer une carte du réseau. Il est largement utilisé par les professionnels de la sécurité et les administrateurs réseau pour évaluer la sécurité des systèmes, identifier les vulnérabilités et effectuer des audits de sécurité.

Nmap utilise des techniques telles que la découverte d'hôtes, le scan de ports, la détection de services, et d'autres méthodes avancées pour collecter des informations sur les systèmes cibles. Il peut être utilisé à des fins légales et éthiques pour renforcer la sécurité des réseaux, mais il est important de noter que l'utilisation non autorisée de Nmap ou d'autres outils similaires peut être contraire à la loi.

Voici une version corrigée et reformulée de votre texte :

"Pourquoi Nmap est-il le meilleur outil de scan ? Il est important de noter que ceci n'est que mon avis personnel, et qu'il existe d'autres outils populaires parmi les experts en cybersécurité. Il est souvent primordial d'utiliser plusieurs outils et de croiser les résultats pour trouver le plus de détails cachés. D'autres outils tels que Nano, Zenmap (qui, à mon avis, est la version la moins sophistiquée) et Angry IP Scanner, sont plus des outils complémentaires à Nmap qu'une véritable alternative. Nous avons choisi Nmap dans le cadre de cet atelier car, à lui seul, l'outil est tellement complet que nous aurions pu accomplir l'intégralité de l'atelier avec lui.

Avant de passer à la phase de démonstration de Nmap, j'aimerais montrer à quel point l'outil est puissant. Les trames TCP ont leur propre système, un peu comme un modèle OSI, une structure similaire à celle des requêtes ARP et des réponses. Les trames TCP ont des drapeaux que les commandes Windows et PowerShell ne permettent pas directement d'identifier.

**URG** : Le drapeau URG (urgent) indique que le champ de pointeur urgent est significatif. Le pointeur urgent indique que les données entrantes sont urgentes et qu'un segment TCP avec le drapeau URG activé est traité immédiatement, sans attendre les segments TCP précédemment envoyés.

**ACK** : Le drapeau d'acquiescement (acknowledgment) indique que le numéro d'acquiescement est significatif. Il est utilisé pour reconnaître la réception d'un segment TCP.

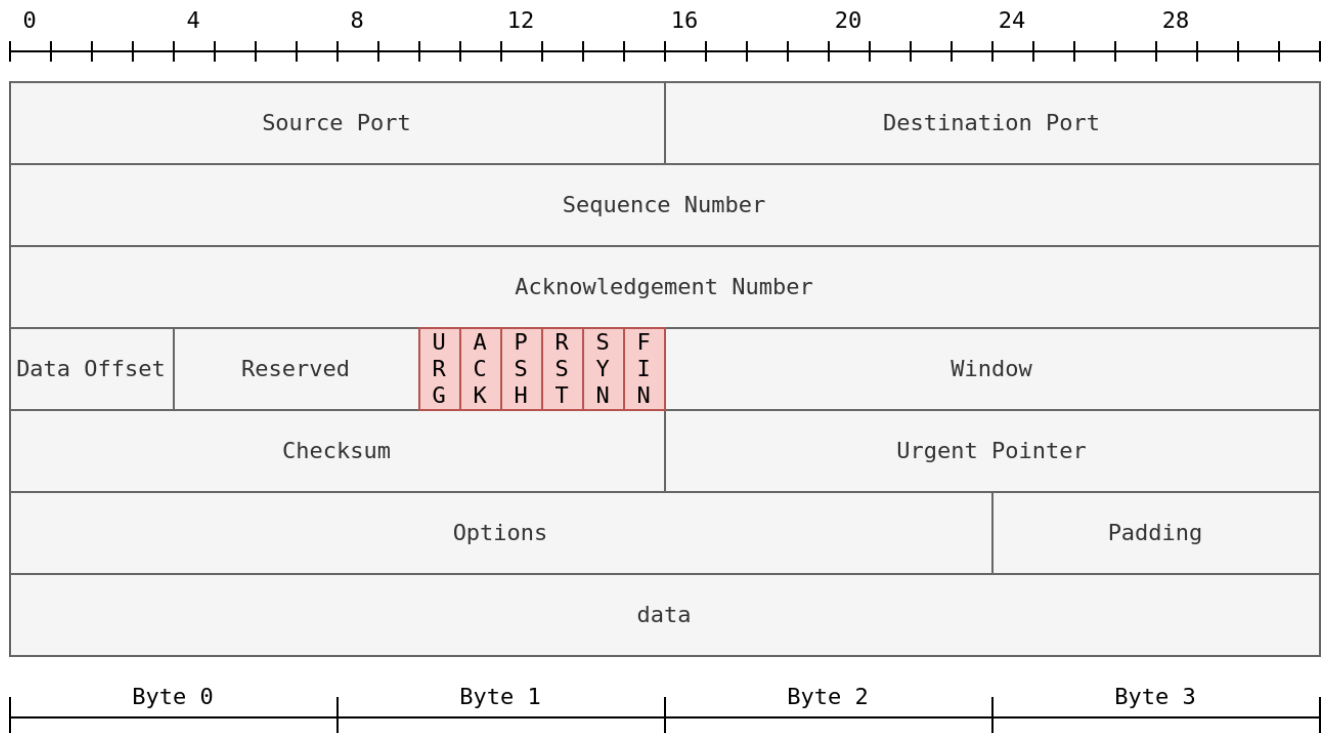
**PSH** : Le drapeau Push demande à TCP de transmettre rapidement les données à l'application.

**RST** : Le drapeau Reset est utilisé pour réinitialiser la connexion. Un autre dispositif, tel qu'un pare-feu, pourrait l'envoyer pour rompre une connexion TCP. Ce drapeau est également utilisé lorsque des données sont envoyées à un hôte et qu'il n'y a aucun service à l'extrémité réceptrice pour répondre.

**SYN** : Le drapeau Synchronize est utilisé pour initier une poignée de main à trois voies (TCP 3-way handshake) et synchroniser les numéros de séquence avec l'autre hôte. Le numéro de séquence doit être défini de manière aléatoire lors de l'établissement d'une connexion TCP.

**FIN** : L'émetteur n'a plus de données à envoyer.

## TCP Header (RFC793)



Nmap -sL 172.31.1.1/24

Identifier les postes utilisés, etc., le nom d'utilisateur, etc. Ici, nous effectuons un scan de base, mais l'avantage de Nmap est que l'on peut cumuler les options à l'infini. Il suffit d'ajouter un -A en majuscule, et nous aurions absolument tous les détails. Je ne l'ai pas fait car j'aurais eu trop d'informations, et cela aurait probablement pris 2 à 3 heures étant donné la taille du réseau.

```
C:\Users\eloha>nmap -sL 172.31.1.1/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-30 12:47 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
Nmap scan report for 172.31.1.22
Nmap scan report for 172.31.1.23
Nmap scan report for 172.31.1.24
Nmap scan report for 172.31.1.25
Nmap scan report for 172.31.1.26
Nmap scan report for AL-Zabbix.sio.local (172.31.1.27)
Nmap scan report for 172.31.1.28
```

On peut également se concentrer sur l'analyse des trames ARP pour forcer le réseau à se redécouvrir.

```
C:\Users\eloha>nmap -PR -sn 172.31.1.52
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-30 12:51 Paris, Madrid
Nmap scan report for S-PROFS01.sio.local (172.31.1.52)
Host is up (0.00s latency).
MAC Address: 74:46:A0:94:0E:47 (Hewlett Packard)
Nmap done: 1 IP address (1 host up) scanned in 5.90 seconds
```

Il est également possible d'identifier les machines virtuelles, les marques de processeurs, ou les équipements réseau, des informations très utiles car certaines vulnérabilités sont communes à des modèles ou des marques spécifiques. Cela permet de mieux comprendre leur fonctionnement.

```
MAC Address: 54:BF:64:FA:15:2A (Dell)
Nmap scan report for al-esxi-02-idrac.sio.local (172.31.1.12)
Host is up (0.0020s latency).
MAC Address: 54:BF:64:FA:13:62 (Dell)
Nmap scan report for al-esxi-03-idrac.sio.local (172.31.1.13)
Host is up (0.0020s latency).
MAC Address: 54:BF:64:FA:0A:74 (Dell)
Nmap scan report for 172.31.1.21
Host is up (0.0010s latency).
MAC Address: 00:C0:FF:44:53:F0 (Seagate Cloud Systems)
Nmap scan report for 172.31.1.22
Host is up (0.0010s latency).
MAC Address: 00:C0:FF:44:6A:C0 (Seagate Cloud Systems)
Nmap scan report for 172.31.1.31
Host is up (0.0010s latency).
MAC Address: 00:11:32:9B:09:25 (Synology Incorporated)
Nmap scan report for 172.31.1.32
Host is up (0.87s latency).
MAC Address: 38:21:C7:4C:DE:A2 (Aruba, a Hewlett Packard Enterprise Company)
Nmap scan report for 172.31.1.34
Host is up (0.035s latency).
MAC Address: CC:B2:55:B9:73:DA (D-Link International)
Nmap scan report for 172.31.1.35
Host is up (0.0020s latency).
MAC Address: B4:39:D6:A7:A5:40 (ProCurve Networking by HP)
Nmap scan report for 172.31.1.36
Host is up (0.080s latency).
MAC Address: F0:62:81:06:90:40 (ProCurve Networking by HP)
Nmap scan report for 172.31.1.37
Host is up (0.15s latency).
```

```
MAC Address: D8:67:D9:D2:4A:C9 (Cisco Systems)
Nmap scan report for 172.31.1.187
Host is up (0.0010s latency).
MAC Address: 60:73:5C:14:C1:53 (Cisco Systems)
Nmap scan report for 172.31.1.188
Host is up (0.0010s latency).
MAC Address: 60:73:5C:14:C0:D5 (Cisco Systems)
Nmap scan report for 172.31.1.189
Host is up (0.0010s latency).
MAC Address: 44:03:A7:E5:E2:AB (Cisco Systems)
Nmap scan report for SRV-SIO.sio.local (172.31.1.250)
Host is up (0.0040s latency).
MAC Address: F8:BC:12:45:60:38 (Dell)
Nmap scan report for 172.31.1.253
Host is up (0.0030s latency).
MAC Address: D8:67:D9:D1:B4:2B (Cisco Systems)
Nmap scan report for 172.31.1.254
Host is up (0.0020s latency).
MAC Address: 00:0C:29:B8:25:53 (VMware)
```

Je me penché pour refaire tout le script en utilisant uniquement nmap en remplacement :

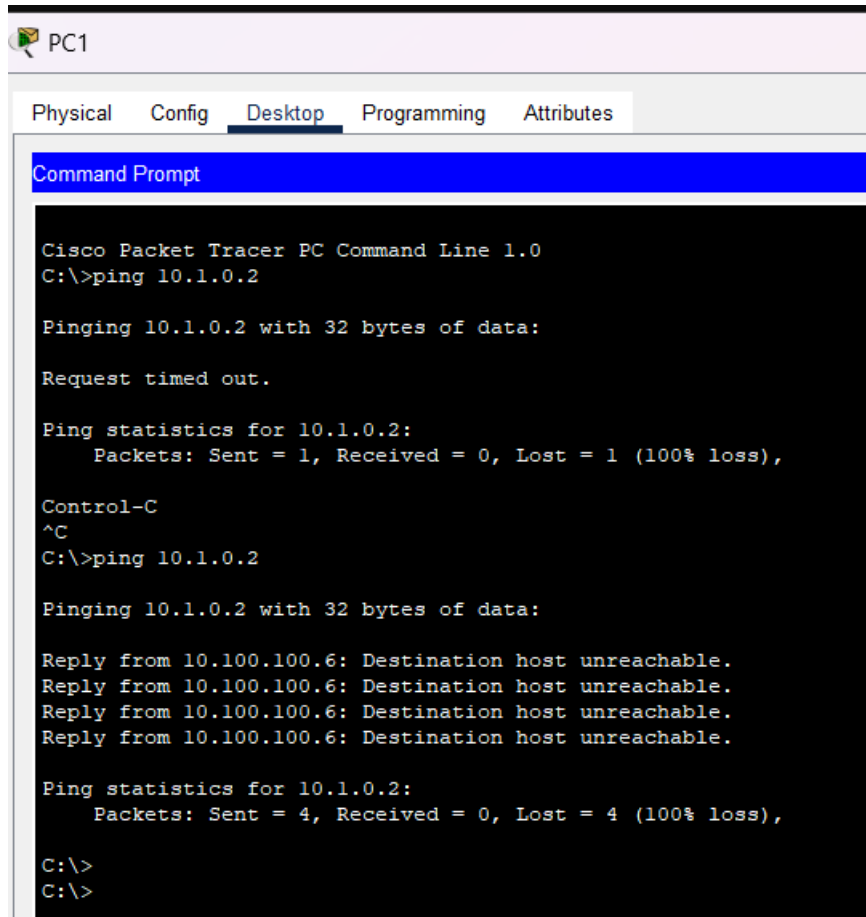
```
1  nmap -sS -A 172.31.1.1/24
2  pause
3  echo "Déterminez si le serveur distant est accessible."
4  echo "Déterminez si le serveur distant est accessible." >> Analyse.txt
5  nmap -sn cisco.com
6  nmap -sn cisco.com >> Analyse.txt
7
8  echo "Test V4"
9  echo "Test V4" >> Analyse.txt
10 echo "Organismes principaux d'Internet"
11 echo "Organismes principaux d'Internet" >> Analyse.txt
12 nmap -p 80,443 www.afrinic.net www.apnic.net www.ripe.net www.lacnic.net www.arin.net >> Analyse.txt
13
14 echo "Test V6"
15 echo "Test V6" >> Analyse.txt
16 nmap -6 -p 80,443 www.afrinic.net www.apnic.net www.ripe.net www.lacnic.net www.arin.net >> Analyse.txt
17
18 echo "Suivre une route vers un serveur distant à l'aide de la commande Tracert"
19 echo "Suivre une route vers un serveur distant à l'aide de la commande Tracert" >> Analyse.txt
20 nmap --traceroute www.cisco.com www.peugeot.fr www.sfr.fr www.cisco.fr google.com >> Analyse.txt
21
22 echo "Effectuer un scan de ports"
23 echo "Effectuer un scan de ports" >> Analyse.txt
24 nmap -p 1-1000 cisco.com >> Analyse.txt
25
26 echo "Découvrir les services en cours d'exécution"
27 echo "Découvrir les services en cours d'exécution" >> Analyse.txt
28 nmap -sV cisco.com >> Analyse.txt
29
30 echo "Identifier le système d'exploitation"
31 echo "Identifier le système d'exploitation" >> Analyse.txt
32 nmap -O cisco.com >> Analyse.txt
33
```

Et finalement avec moins de commande on a un résultat plus complet sur certains points même si il manque un ou deux résultats forcément.

Mais pour l'utilisation d'une seule commande je trouve ça louable.

**XIX. Packet tracer**

La commande nous aide à visualiser et résoudre des problèmes en tant que technicien. Par exemple, l'utilisation de la commande tracer nous permet de localiser précisément l'endroit où un problème de connexion se produit.



The screenshot shows the Cisco Packet Tracer PC Command Line interface for PC1. The 'Desktop' tab is selected. The Command Prompt displays the following text:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.1.0.2

Pinging 10.1.0.2 with 32 bytes of data:

Request timed out.

Ping statistics for 10.1.0.2:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

Control-C
^C
C:\>ping 10.1.0.2

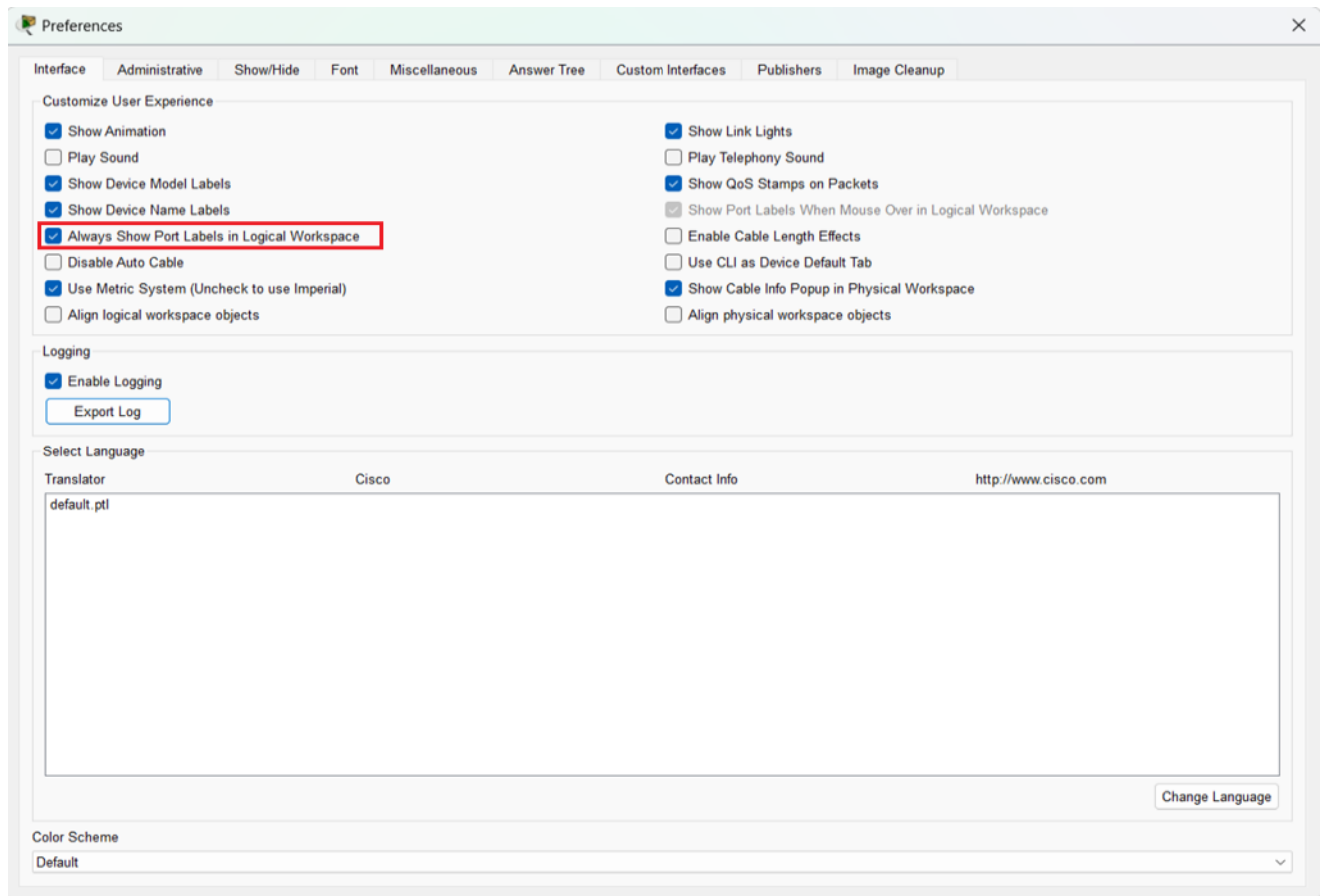
Pinging 10.1.0.2 with 32 bytes of data:

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.

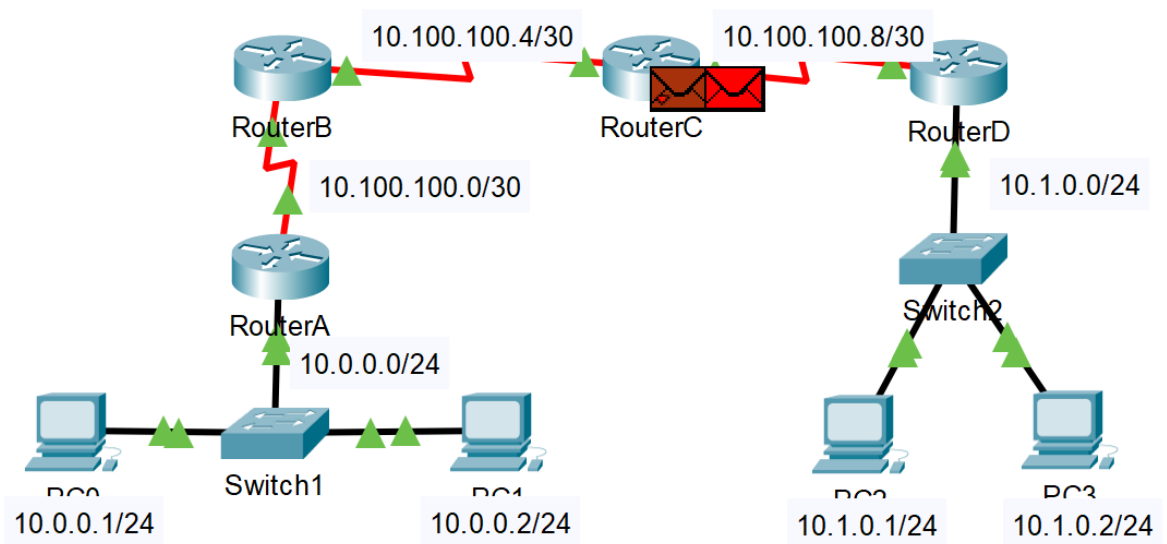
Ping statistics for 10.1.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
C:\>
```

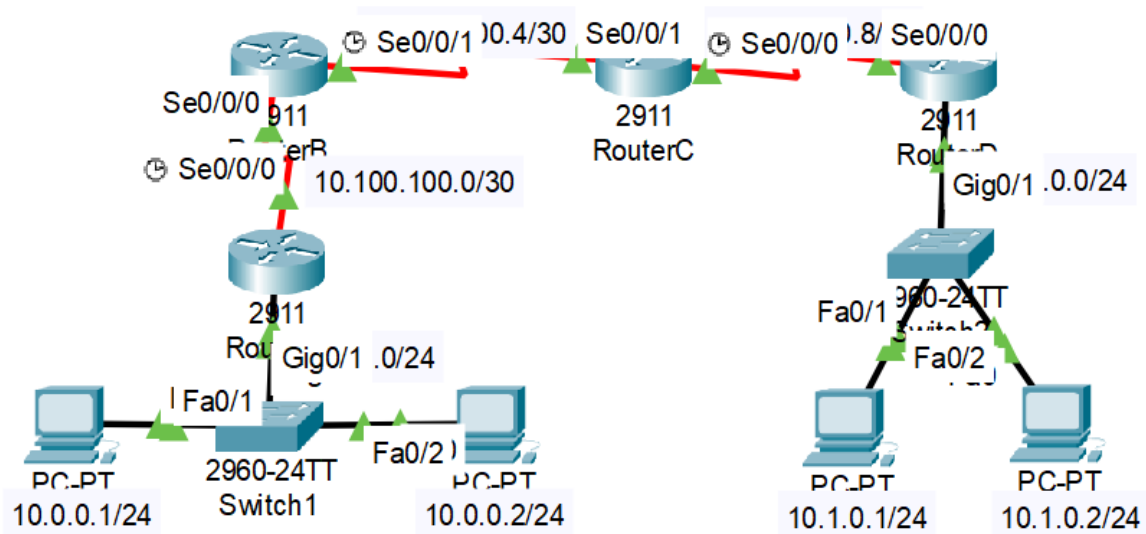
Avant de continuer les modifications, nous allons activer une option très utile qui permettra de visualiser les interfaces, car vous avez bloqué toute interaction possible avec la topologie.



Ce qui nous permet de passer de ceci :



à cela :



Personnellement, je n'utilise pas "tracert" car il existe des outils plus performants tels que l'outil d'enveloppe de trame de paquets, qui offre une efficacité accrue. Bien que fonctionnant de manière similaire, cette alternative permet une visualisation directe en interface graphique, indiquant clairement l'emplacement du problème. Dans notre cas, nous avons identifié que le souci résidait au niveau de l'interface SE/0/0/0 du routeur C en raison d'une adresse non valide. Après avoir effectué le changement avec ce marqueur, tout est maintenant opérationnel. Si on fait un show running-config sur le routeur C on se rend compte que l'interface n'est pas valide sur le port serial 0/0/0

```
RouterC(config-if)#ip address 10.100.100.9 255.255.255.252
RouterC(config-if)#
```

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	PC2	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC3	PC1	ICMP		0.000	N	1	(edit)	(delete)



**XX. Routage dynamique :**

Le routage dynamique est un processus automatisé par lequel les routeurs d'un réseau échangent automatiquement des informations sur les chemins disponibles vers les différentes destinations. Ces informations de routage permettent aux routeurs de prendre des décisions sur la meilleure façon de faire parvenir les paquets de données à leur destination, en fonction des conditions du réseau. Contrairement au routage statique, où les chemins sont configurés manuellement, le routage dynamique s'adapte aux changements de la topologie du réseau de manière automatique. Les protocoles de routage, tels que OSPF, EIGRP, et RIP, sont souvent utilisés pour faciliter le routage dynamique.

OSPF est significativement plus sécurisé, mais sa configuration est plus complexe. Pour un petit réseau tel que celui-ci, RIP est amplement suffisant.

Il suffit de faire c'est commande ensuite :

```
RouterA>enable
```

```
RouterA#configure terminal
```

```
RouterA(config)#router rip
```

```
RouterA(config-router)#version 2
```

```
RouterA(config-router)#network 10.0.0.0
```

```
RouterA(config-router)#network 10.100.100.0
```

```
RouterA(config-router)#exit
```

```
RouterB>enable
```

```
RouterB#configure terminal
```

```
RouterB(config)#router rip
```

```
RouterB(config-router)#version 2
```

```
RouterB(config-router)#network 10.100.100.0
```

```
RouterB(config-router)#network 10.100.100.4
```

```
RouterB(config-router)#network 10.1.0.0
```

```
RouterB(config-router)#exit
```

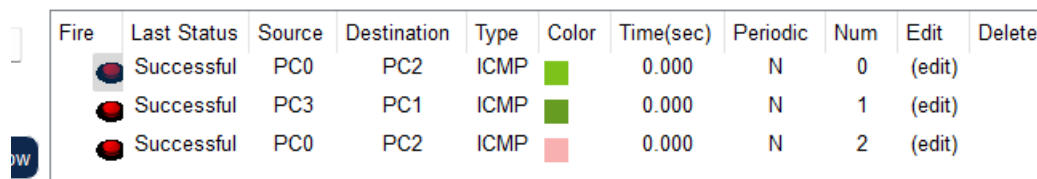
```
RouterC>enable
```

```
RouterC#configure terminal
```

```
RouterC(config)#router rip
```

```
RouterC(config-router)#version 2
RouterC(config-router)#network 10.100.100.4
RouterC(config-router)#network 10.100.100.8
RouterC(config-router)#network 10.1.0.0
RouterC(config-router)#exit
```

```
RouterD>enable
RouterD#configure terminal
RouterD(config)#router rip
RouterD(config-router)#version 2
RouterD(config-router)#network 10.1.0.0
RouterD(config-router)#network 10.100.100.8
RouterD(config-router)#exit
```



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	PC2	ICMP		0.000	N	0	(edit)	
	Successful	PC3	PC1	ICMP		0.000	N	1	(edit)	
	Successful	PC0	PC2	ICMP		0.000	N	2	(edit)	

## XXI. Conclusion :

Au cours de cet atelier, nous avons acquis la compétence de concevoir des cryptages compatibles avec différents systèmes d'exploitation. Nous avons également maîtrisé la réalisation d'une OSINT, une étape cruciale pour obtenir des informations sur une entreprise, comprendre notre réseau, et identifier les problèmes qu'ils soient internes ou externes. Ce TP constitue une introduction au pentest et à l'analyse passive.

**XXII. Annexe :****n) Commande à retenir**

Objectif:	Commande :
<b>Gestion réseau</b>	
Voir la configuration IP	Ipconfig /all
Renouveler l'adresse IP	ipconfig /renew
Vérifier la connectivité réseau	ping [adresse IP ou nom de domaine]
Traceroute vers une destination	tracert [adresse IP ou nom de domaine]
Vérifier les ports ouverts sur une machine	netstat -an
<b>Commandes Linux</b>	
Rechercher des motifs dans un fichier	grep [motif] [nom du fichier]
Télécharger un fichier depuis Internet	curl -O [URL du fichier]
Analyser les ports d'une mach	nmap [adresse IP]
<b>Commandes Windows</b>	
Afficher la configuration réseau	netsh interface ip show config
Afficher les interfaces réseau	netsh interface show interface
Réinitialiser l'interface réseau	netsh interface reset
Changer l'adresse IP	netsh interface ip set address "Nom de l'interface" static [Adresse IP] [Masque de sous-réseau] [Passerelle] [Métrique]
Configurer un serveur DNS	netsh interface ip set dns "Nom de l'interface" static [Adresse DNS primaire] validate=no
Configurer le proxy	netsh winhttp set proxy proxy-server="http=proxy.example.com:8080;https=proxy.example.com:8080" bypass-list="*.example.com"
Activer/désactiver ICS	netsh sharing set hostednetwork mode=allow (activer)
<b>Sécurité réseau</b>	
Vérifier les connexions réseau actives	netstat -an
Vérifier les règles du pare-feu	netsh advfirewall show allprofiles
Analyser le trafic réseau	tcpdump (Linux) ou Wireshark (interface graphique)
<b>Administration système</b>	
Afficher les informations	systeminfo

système	
Gérer les services	services.msc
Gérer les utilisateurs	net user
Afficher la table ARP	arp -a
Supprimer une entrée de la table ARP	arp -d [adresse IP]

**o) Protocoles vus**

Protocoles :		
Protocole :	Ports	Description
<b>TCP</b>	0-65535	Assure une transmission fiable des données en établissant une connexion et en gérant la séquence d'échange.
<b>SSH</b>	22	Permet une connexion sécurisée à distance en chiffrant les communications entre les deux points.
<b>RCPBIND</b>	111	Associe les numéros de port RPC (Remote Procedure Call) aux services correspondants sur un système.
<b>HTTP</b>	80	Protocole de transfert hypertexte utilisé pour le transfert de données sur le World Wide Web.
<b>HTTPS</b>	443	Version sécurisée de HTTP, crypte les données pour assurer une communication web sécurisée.
<b>UDP</b>	0-65535	Protocole de datagramme utilisateur, offre une communication plus rapide mais non fiable sans établir de connexion.
<b>DNS</b>	53	Traduit les noms de domaine en adresses IP, facilitant la navigation sur Internet.
<b>DHCP</b>		Permet l'attribution dynamique d'adresses IP aux dispositifs sur un réseau, simplifiant la configuration réseau. Haut du formulaire
<b>FTP</b>		
<b>ARP</b>		Protocole qui mappe une adresse IP à une adresse physique (MAC) dans un réseau local, facilitant la communication au niveau de la couche de liaison de données.
<b>IPv4</b>		Protocole de réseau qui attribue des adresses uniques à chaque appareil connecté à Internet pour faciliter l'acheminement des données.
<b>IPv6</b>		Version améliorée d'IPv4, utilisée pour résoudre la pénurie d'adresses en attribuant un identifiant unique à un nombre considérablement plus grand d'appareils connectés à Internet

## p) Langage abordé

**Langage :**

Langage :	Date de création	Description	Utilisations Courantes
Python	1991	Langage de programmation polyvalent, favorisé pour sa lisibilité et sa simplicité.	Développement web, automatisation de tâches.
Batch	1980	Langage de script utilisé principalement sous les systèmes d'exploitation Windows pour automatiser des tâches.	Scripts de traitement par lots.
Powershell	2006	Langage de script et de shell développé par Microsoft, privilégié pour l'automatisation des tâches système.	Administration système, scripts d'automatisation

## q) Librairie :

**Librairie :**

Langage :	Description	Avantage
Tkinter	Interface graphique pour Python.	Intégration native avec Python, simplifiant le développement GUI.
subprocess	Permet d'exécuter des commandes système.	Facilite l'exécution de commandes système et la communication entre processus.
threading	Facilite la programmation multithread en Python.	Amélioration des performances grâce à l'exécution concurrente de tâches.
Os	Fournit des fonctionnalités liées au système d'exploitation.	Abstraction efficace pour les opérations système courantes.
shodan	Permet d'accéder à l'API Shodan pour la recherche et l'exploration de dispositifs connectés à Internet.	Offre une large gamme de fonctionnalités pour la découverte d'appareils, la collecte d'informations sur les services, et la surveillance de la sécurité en ligne.

### XXIII. Sources :

<https://www.shodan.io/host/91.220.197.80>

<https://www.whois.com/whois/btssio.org>

<https://www.rfc-editor.org/rfc/rfc826>

<https://www.kali.org/>

<https://tryhackme.com/room/nmap01>

<https://tryhackme.com/room/nmap02>

<https://tryhackme.com/room/nmap03>

<https://www.frameip.com/routage/>

<https://www.it-connect.fr/cisco-configuration-du-routage-rip/>