

# Rapport de TP Sécurité- Deuxième partie

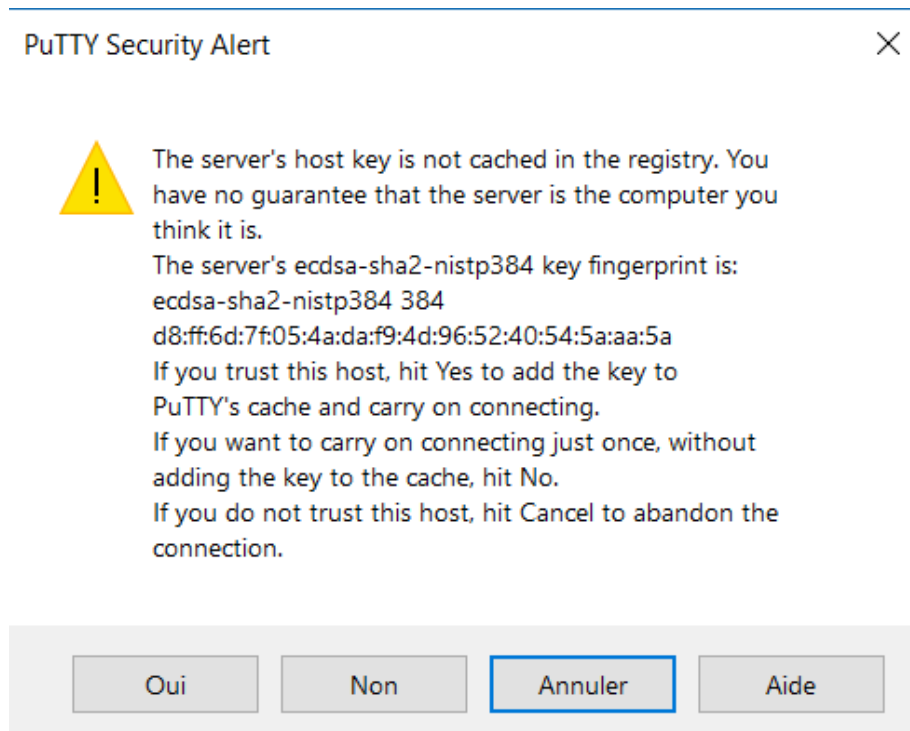
## Table des matières

Troisième TP : Administration SSH (Première partie) .....	2
Objectif 1 : .....	2
Objectif 2 : .....	4
Quatrième TP : Administration SSH (Deuxième partie) .....	5
Tunnel SSH : .....	7
Cinquième TP : Syslog.....	9
Vérification de la réception des logs .....	10
Recherche / Identification (comprendre les niveaux de gravité...).....	11
Paramétrage et émission d'alertes (exemple Mail) .....	12
Rotation des fichiers de log.....	13
Sixième TP : Découverte des Scanners.....	14
Angry IP Scanner.....	14
Advanced IP Scanner .....	16
Septième TP : Écoute et Analyse du réseau .....	16
Étape #1.....	16
Étape #2.....	18
Étape #3.....	19

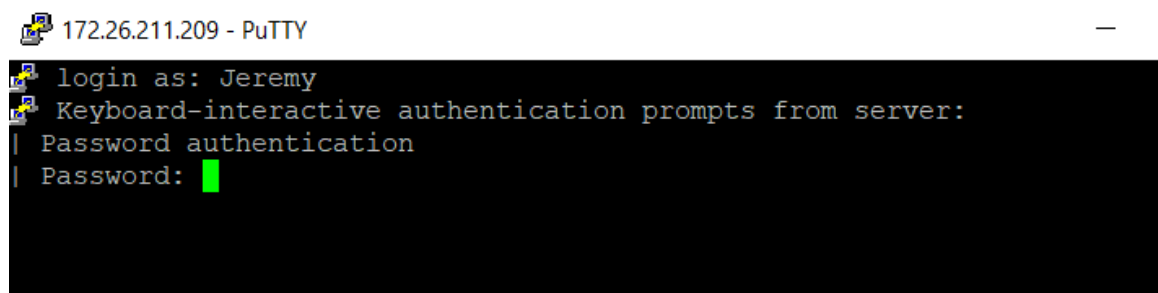
## Troisième TP : Administration SSH (Première partie)

Pour ce TP je travaille sur un seul ordinateur physique Windows.

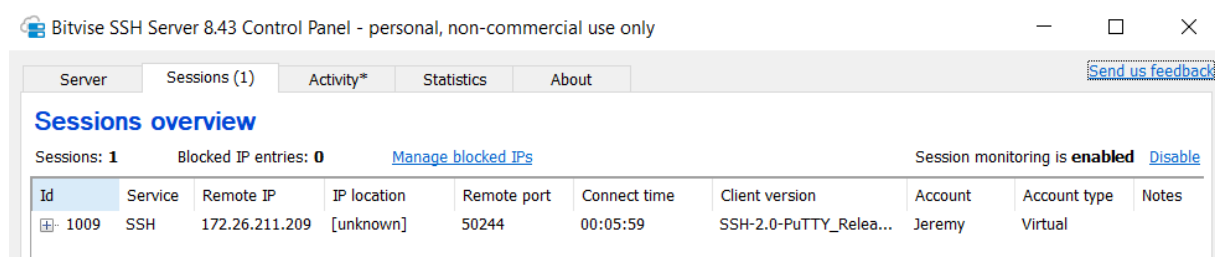
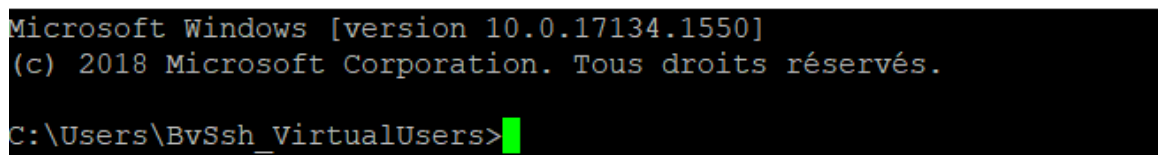
### Objectif 1 :



On essaye de se connecter grâce à PuTTY au serveur SSH, mais comme il ne connaît pas l'hôte il nous prévient qu'il peut s'agir d'une machine inconnue, cependant on peut ajouter la clé de l'hôte afin de se connecter plus facilement.



Une fois qu'on a rentré l'adresse IP dans PuTTY on peut se connecter à notre serveur SSH en rentrant notre MDP en utilisant le nom d'utilisateur que l'on a inscrit plus tôt.



Comment on peut le voir dans notre serveur la connexion entre le client et le serveur est effectué.

## Objectif 2 :

PuTTY Key Generator ? X

File Key Conversions Help

**Key**

Public key for pasting into OpenSSH authorized\_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAQEAwwbOTD7cxw48TiLtgsb9JCCXLw69DVsgUyyqGibO
ewynufZR2Rh3qsnL9v0o8QpLhIrMoNOeyi83nvMPM1kVnbKwcPM3JUg8dlmxcftgAetKdlQbQf
+0FEkGaBn5Sw9PI5XrGJiKZhsPzqTko+QG8I997sHjUWtwfO+oBr9hbJCDmr5G52HX7WDK
+JhW6vUOglm3OVu9AeEPPI5dIH78wlHiGCz0Td823FLAypQS9Kjh2Srts/QDNdcCdoHdHN
```

Key fingerprint: ssh-rsa 2048 91:26:e0:06:53:8c:1e:fc:ab:7f:01:d6:a5:2e:75:fe

Key comment: rsa-key-20200627

Key passphrase: ●●●●●●●●

Confirm passphrase: ●●●●●●●●

**Actions**

Generate a public/private key pair Generate

Load an existing private key file Load

Save the generated key Save public key Save private key

**Parameters**

Type of key to generate:

☒ RSA ☐ DSA ☐ ECDSA ☐ Ed25519 ☐ SSH-1 (RSA)

Number of bits in a generated key: 2048

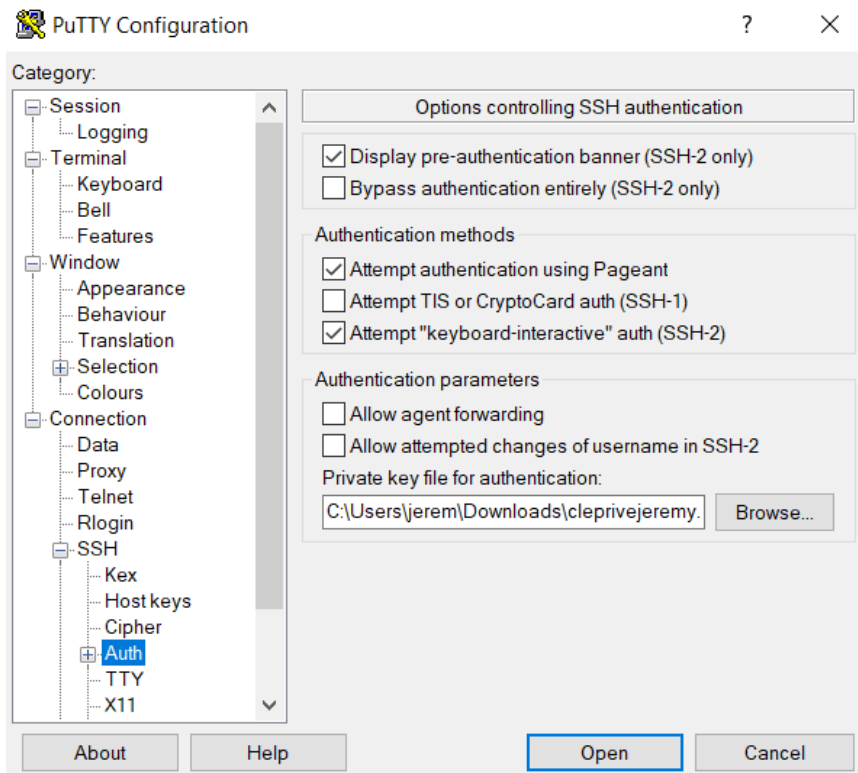
On utilise PuTTY Gen afin de générer une clef publique et privé afin les importer dans PuTTY et Bitvise.

Public keys | Cryptographic provider: Windows CNG (x86) with additions — □ X

You have imported the following public keys:

Algorithm	Size	MD5 Fingerprint	Bubble Babble	SHA-256 Fingerprint	Insert time	Comment
Public keys supported by the current crypto provider (1):						
RSA	2048	91:26:e0:06:53:8c:1e:fc:ab:7f:01:d6:a5:2e:75:fe	xihid-kykip-vonof-...	MwwCo2tW9f0a1jyIM3NF2n...	2020-06-27 11:57	"rsa-key-20200627"

Dans Bitvise on ajoute la clé privée dans notre serveur SSH.



Enfin dans PuTTY on ajoute la clé privée que l'on a généré précédemment.

192.168.0.6 - PuTTY

```
Using username "Jeremy".
Authenticating with public key "rsa-key-20200627"
Passphrase for key "rsa-key-20200627":
```

Maintenant, on lance la connexion entre le client et le serveur, désormais le serveur requière la passphrase qu'on a ajouté plus tôt.

192.168.0.6 - PuTTY

```
Microsoft Windows [version 10.0.17134.1550]
(c) 2018 Microsoft Corporation. Tous droits réservés.

C:\Users\BvSsh_VirtualUsers>
```

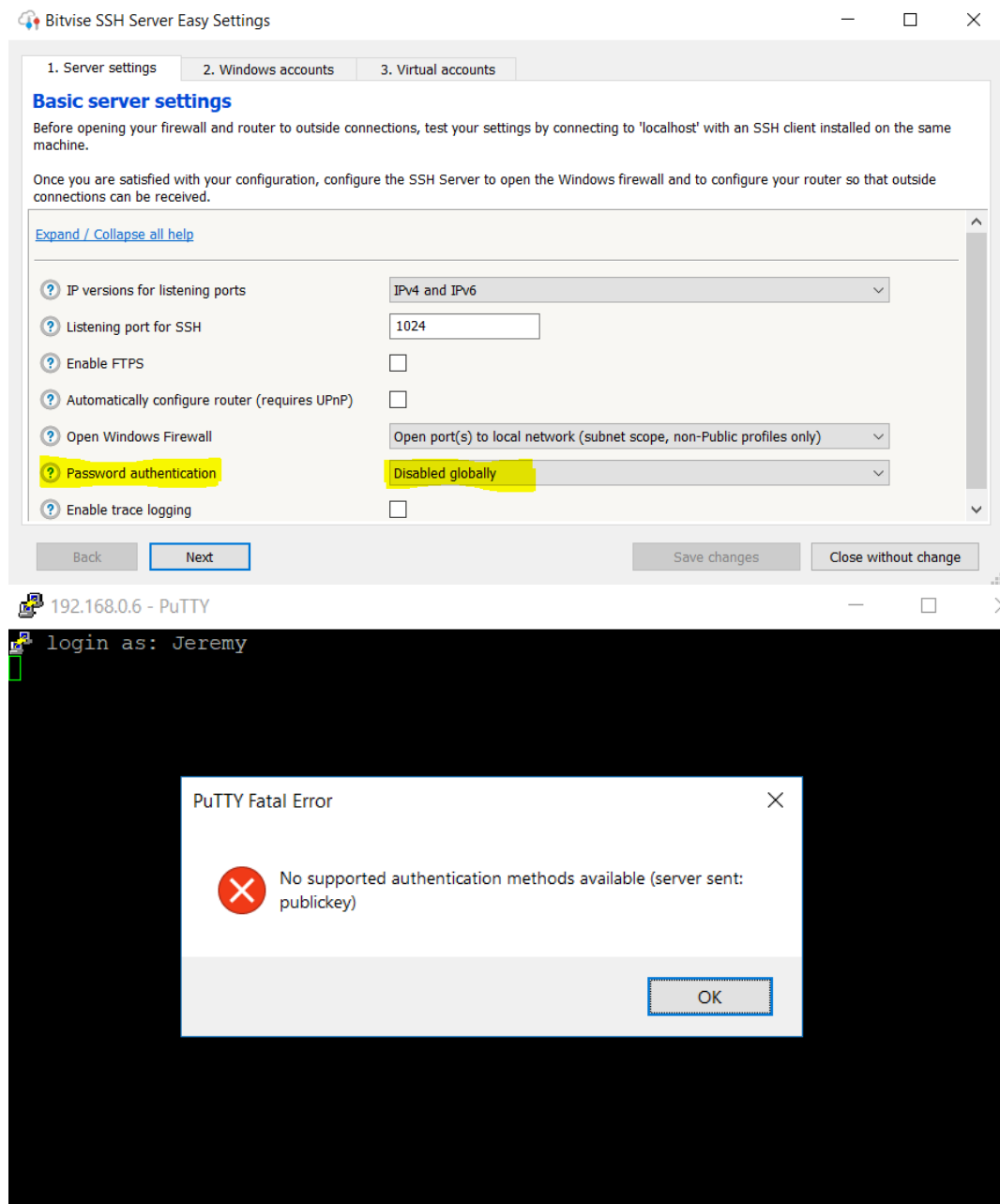
Une clé privée nous permet de nous connecter de manière plus sécuriser sans avoir à retenir plusieurs mots de passe par serveur, ici on a juste à posséder la passphrase pour se connecter.

On peut également désactiver la connexion par mot de passe pour plus de sécurité.

## Quatrième TP : Administration SSH (Deuxième partie)

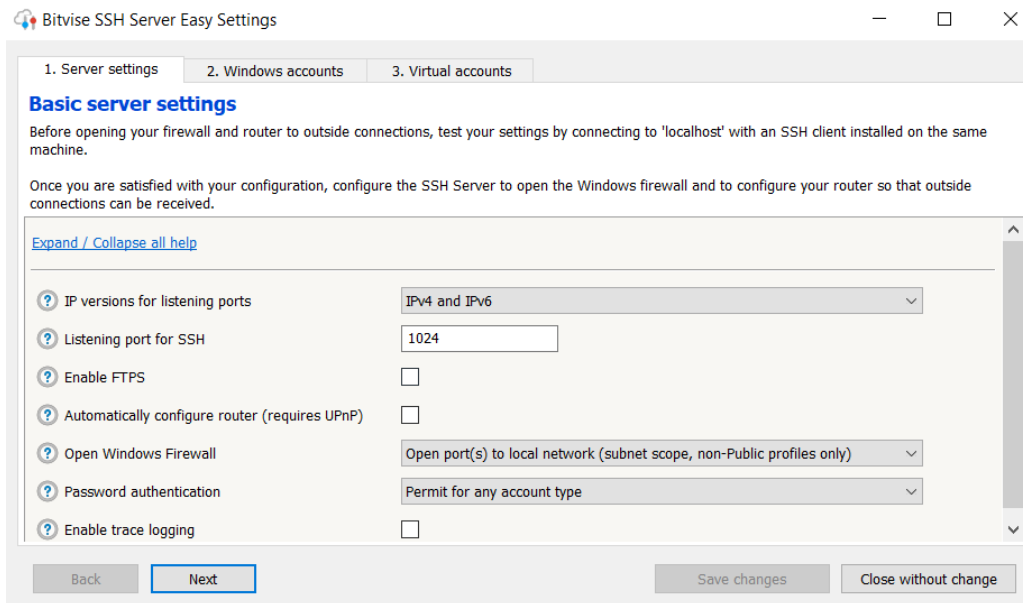
Il existe de nombreuses optimisations possibles :

1. Désactiver la connexion par mot de passe :

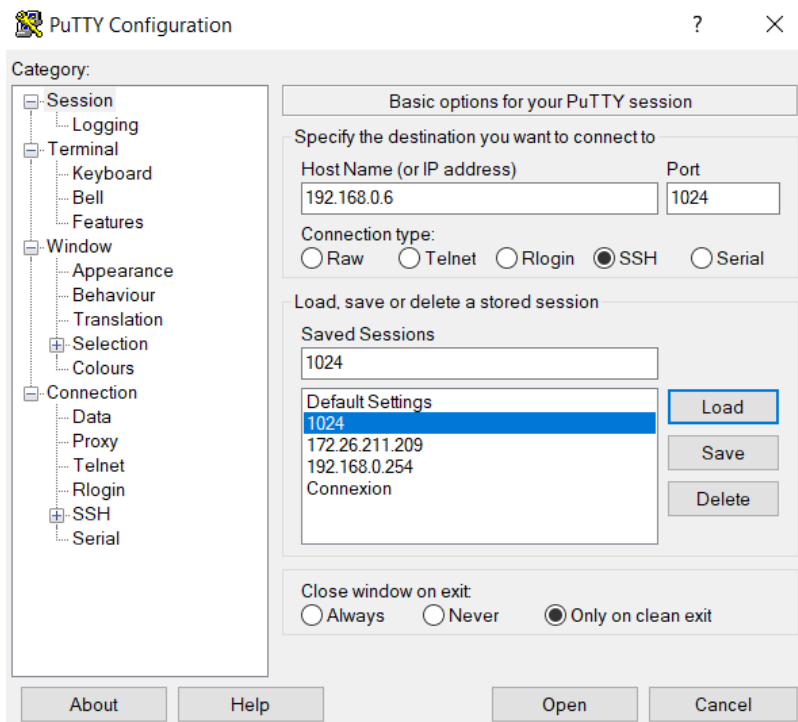


Jusqu'alors la connexion par MDP était possible cependant on peut faire sorte que cela ne soit plus possible, dans les options de notre serveur on peut désactiver la connexion par MDP.

## 2. Changer le port de connexion

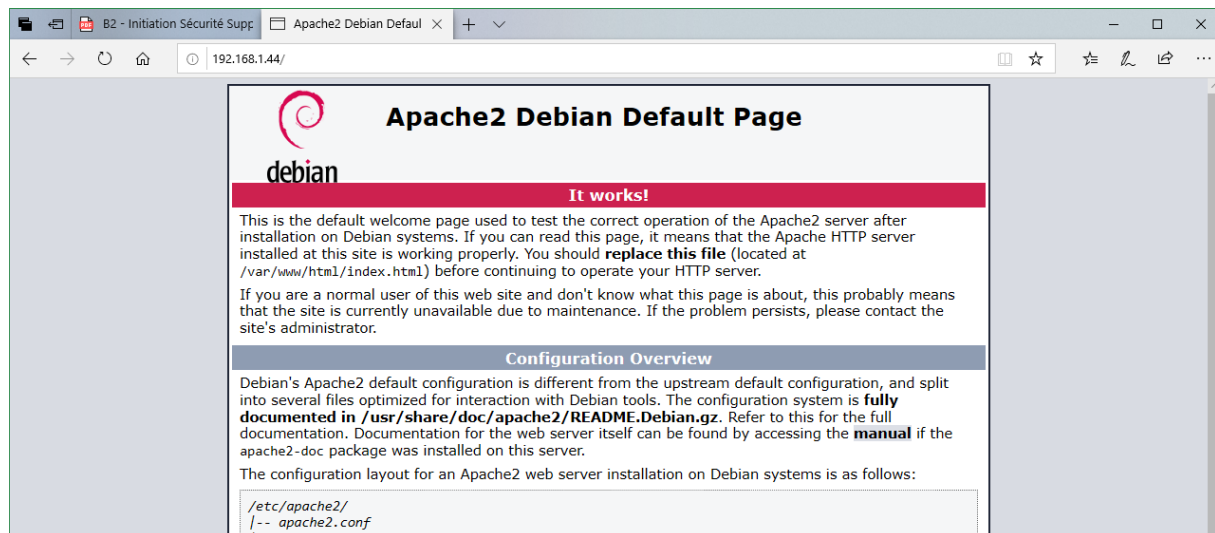


Dans notre serveur SSH on peut paramétrer le port d'écoute ici j'ai choisi le port 1024.

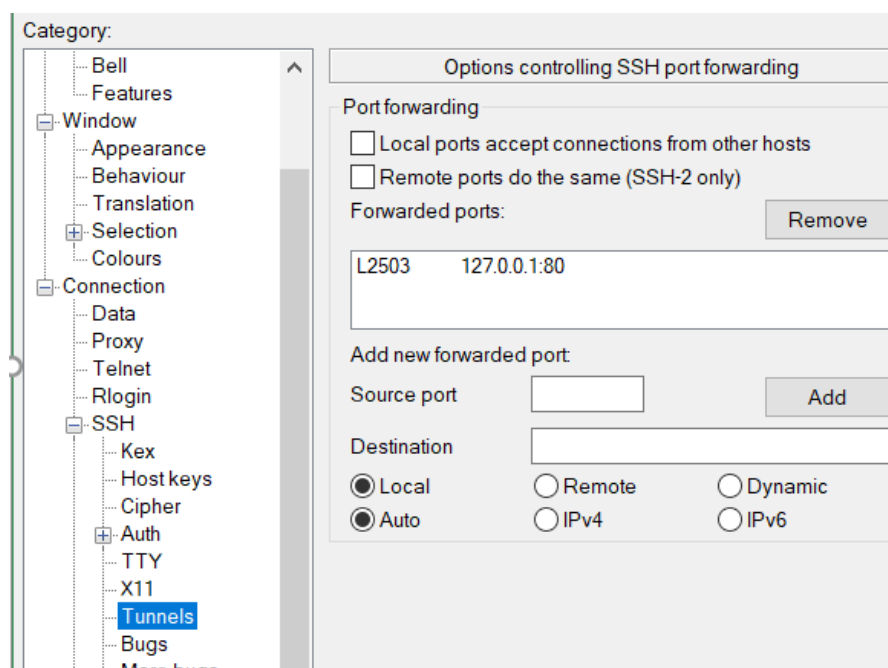


Enfin dans PuTTY on a juste à changer le port par celui correspondant au serveur.

Tunnel SSH :



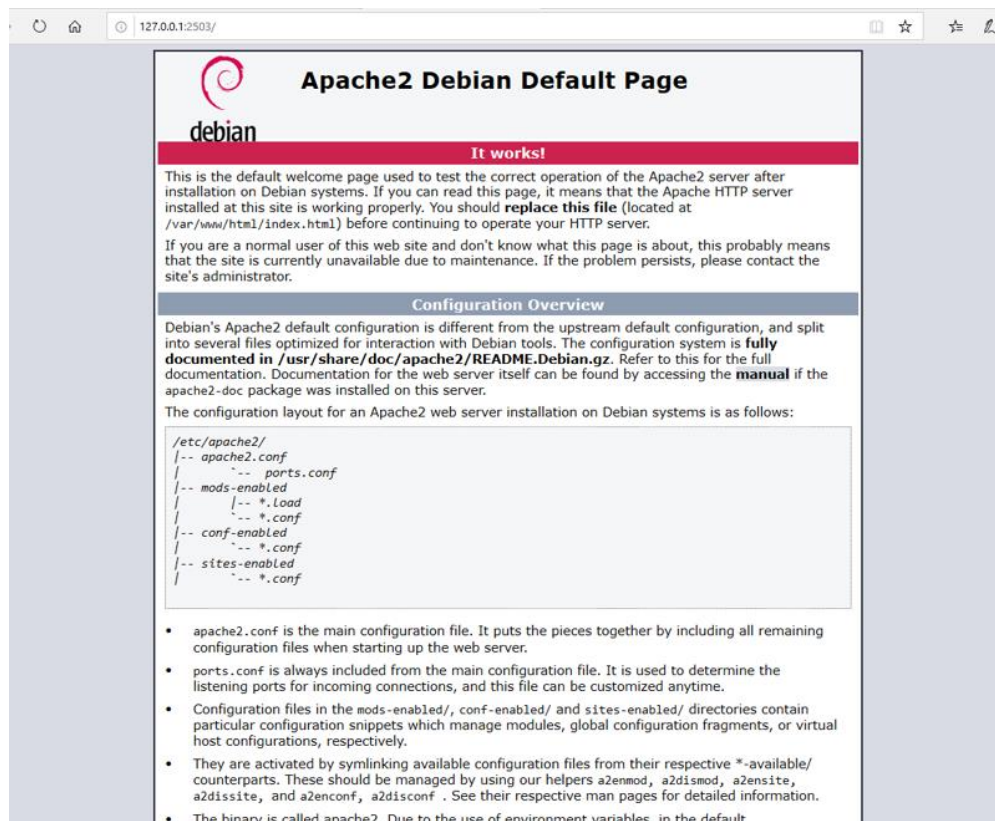
J'ai installé apache2 afin de simuler un serveur, nous allons utiliser un tunnel afin de faire de la redirection sur ce serveur afin de simuler un localhost.



Tout d'abord, dans PuTTY on configure notre tunnel.

Nous allons utiliser le port source 2503 afin de faire de la redirection.



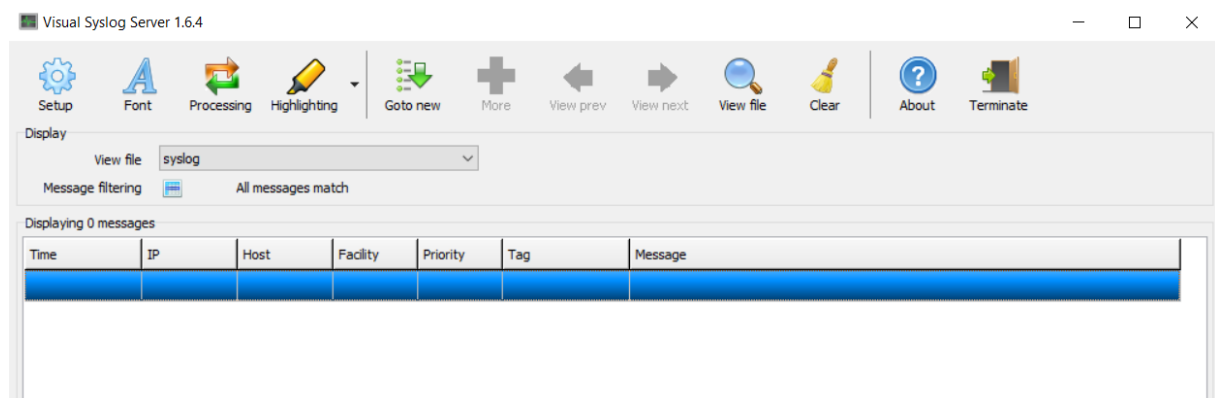


On voit bien que la connexion a eu lieu grâce au tunnel mis en place précédemment.

Le tunneling est un protocole de communication qui permet le transfert de données d'un réseau à un autre. Il permet d'envoyer des communications sur un réseau privé à travers un réseau public, ce processus s'appelle l'encapsulation. Dans ce processus d'encapsulation, les paquets de données apparaissent comme s'ils étaient de nature publique sur un réseau public alors qu'en réalité ils sont considérés comme des paquets de données privés. Cela leur permet de passer inaperçus.

L'avantage de créer un tunnel SSH est qu'il permet de crypter et d'anonymiser les flux entre le client SSH et le serveur (ce qui représente une alternative à un VPN).

## Cinquième TP : Syslog



Le serveur Syslog nous permettra de gérer les logs et événements qui vont se produire.

```

C:\Windows\system32>evtsys -i -h 192.168.0.6 -f local0 -t server1 -l 0
Command completed successfully

C:\Windows\system32>net start evtsys

Le service Eventlog to Syslog a démarré.

```

Ensuite on installe Evtshys qui permet de transférer les événements vers notre serveur Syslog (-i Install service ; -h host Name of log host(s) ; f facility Facility level of syslog message).

## Vérification de la réception des logs

Visual Syslog Server 1.6.4

Setup Font Processing Highlighting Goto new More View prev View next View file Clear About Terminate

Display View file syslog Message filtering All messages match

Displaying 10 messages

Time	IP	Host	Facility	Priority	Tag	Message
Jun 27 22:25:55	192.168.0.6	LAPTOP-V3FDQ	local0	notice	server1	Eventlog to Syslog Service Started: Version 4.5.1 (64-bit)
Jun 27 22:25:55	192.168.0.6	LAPTOP-V3FDQ	local0	notice	server1	Flags: LogLevel=0, IncludeOnly=False, EnableTcp=False, IncludeTag=True, StatusInterval=0
Jun 27 22:27:49	192.168.0.6	LAPTOP-V3FDQ	local0	notice	server1	Security-SPP: 16394: La migration de bas niveau hors connexion a réussi.
Jun 27 22:27:49	192.168.0.6	LAPTOP-V3FDQ	local0	notice	server1	Security-SPP: 1003: Le service de protection logicielle a terminé la vérification du statut des lic
Jun 27 22:27:49	192.168.0.6	LAPTOP-V3FDQ	local0	notice	server1	Security-SPP: 1003: Le service de protection logicielle a terminé la vérification du statut des lic
Jun 27 22:27:49	192.168.0.6	LAPTOP-V3FDQ	local0	notice	server1	Security-SPP: 1003: Le service de protection logicielle a terminé la vérification du statut des lic
Jun 27 22:27:49	192.168.0.6	LAPTOP-V3FDQ	local0	notice	server1	Security-SPP: 1003: Le service de protection logicielle a terminé la vérification du statut des lic
Jun 27 22:28:19	192.168.0.6	LAPTOP-V3FDQ	local0	notice	server1	Security-SPP: 16384: La planification du redémarrage du service de protection logicielle à 2120
Jun 27 22:28:31	192.168.0.6	LAPTOP-V3FDQ	local0	notice	server1	Security-Auditing: 4624: AUDIT_SUCCESS L'ouverture de session d'un compte s'est correctem
Jun 27 22:28:31	192.168.0.6	LAPTOP-V3FDQ	local0	notice	server1	Security-Auditing: 4672: AUDIT_SUCCESS Privilèges spéciaux attribués à la nouvelle ouverture

UDP 0.0.0.0:514 TCP 0.0.0.0:514 101

Après cette mise en place, on remarque que notre serveur Syslog reçoit bien les logs.

Message content

```

Time: Jun 27 22:36:01
IP: 192.168.0.6
Host: LAPTOP-V3FDQ78
Facility: local0
Priority: notice
Tag: server1
Message: Security-Auditing: 4624: AUDIT_SUCCESS L'ouverture de session d'un compte s'est correctement
déroulée. Objet : ID de sécurité : S-1-5-18 Nom du compte : LAPTOP-V3FDQ78$ Domaine du compte :
WORKGROUP ID d'ouverture de session : 0x3E7 Informations d'ouverture de session : Type d'ouverture de
session : 5 Mode administrateur restreint : - Compte virtuel : Non Jeton élevé : Oui Niveau d'emprunt
d'identité : Emprunt d'identité Nouvelle ouverture de session : ID de sécurité : S-1-5-18 Nom du compte :
Système Domaine du compte : AUTORITE NT ID d'ouverture de session : 0x3E7 ID d'ouverture de session
liée : 0x0 Nom du compte réseau : - Domaine du compte réseau : - GUID d'ouverture de session :
{00000000-0000-0000-0000-000000000000} Informations sur le processus : ID du processus : 0x3b4 Nom
du processus : C:\Windows\System32\services.exe Informations sur le réseau : Nom de la station de travail
: - Adresse du réseau source : - Port source : - Informations détaillées sur l'authentification : Processus
d'ouverture de session : Advapi Package d'authentification : Negotiate Services en transit : - Nom du package
(NTLM uniquement) : - Longueur de la clé : 0 Cet événement est généré lors de la création d'une ouverture

```

 OK

Ici par exemple, nous avons un log de connexion à un compte, on y retrouve l'heure de connexion, l'adresse IP, le nom d'hôte, la priorité et un message.

## Recherche / Identification (comprendre les niveaux de gravité...)

Visual Syslog Server 1.5.0

Setup Font Processing Highlighting Goto new Previous View file Clear screen About Terminate

Display

View file: syslog the last 1.0 Mb of the 316.7 Mb

Message filtering: All messages match

Displaying 7361 messages of 7369

Time	IP	Host	Facility	Priority	Tag	Message
Dec 18 11:22:32	192.168.1.2		daemon	err	tinyproxy[9409]	readbuff: recv() error "Connection reset by peer"
Dec 18 11:22:33	192.168.1.2		daemon	err	tinyproxy[9456]	read_request_line: Client (file descriptor: 5) closed
Dec 18 11:22:33	192.168.1.2		daemon	err	tinyproxy[9456]	Error reading readable client_fd 5
Dec 18 11:22:33	192.168.1.2	host1	daemon	warning	tinyproxy[9456]	Could not retrieve request entity
Dec 18 11:22:35	192.168.1.1	host1	mail	warning	postfix/smtpd[5589]	warning: hostname 93-179-64-10.ip-msk-ix.p3.ru c
Dec 18 11:22:35	192.168.1.1	host1	mail	info	postfix/smtpd[5589]	connect from unknown[93.179.64.10]
Dec 18 11:22:36	192.168.1.1	host1	mail	info	postfix/smtpd[5589]	NOQUEUE: reject: RCPT from unknown[93.179.64.10]
Dec 18 11:22:36	192.168.1.1	host1	mail	info	postfix/smtpd[5589]	disconnect from unknown[93.179.64.10]

UDP 0.0.0.0:514 TCP 0.0.0.0:514 [1]

Il existe différent type de gravités, certains sont juste là pour fournir une information mais d'autres peuvent prévenir de problème plus grave (erreur de fonctionnement, système inutilisable...) :

Code	Gravité	Mot-clé	Description
0	Emergency	emerg (panic)	Système inutilisable.
1	Alert	alert	Une intervention immédiate est nécessaire.
2	Critical	crit	Erreur critique pour le système.
3	Error	err (error)	Erreur de fonctionnement.
4	Warning	warn (warning)	Avertissement (une erreur peut intervenir si aucune action n'est prise).
5	Notice	notice	Événement normal méritant d'être signalé.
6	Informational	info	Pour information.
7	Debugging	debug	Message de mise au point.

## Paramétrage et émission d'alertes (exemple Mail)

Setup

✕

Main Files E-mail

Smtip server

Address: smtp.gmail.com Port: 465 SSL: SSL Select smtp server: Gmail, iCloud Mail, @mail.ru, yandex

Username: jeremy.deblaecker@gmail.com Password: \*\*\*\*\*

Message

Sender address: amy.deblaecker@gmail.com Sender name: Jeremy DEBLAECKER Recipient address (default): amy.deblaecker@gmail.com

Subject: Alert : {tag} / {host} / {ip}

Message: {time} {message}

Send test message

OK Cancel

Nous allons maintenant paramétrer notre serveur afin de recevoir par email les différentes alertes dans nos logs.

## ← Accès moins sécurisé des applications

Certaines applications et certains appareils utilisent une technologie de connexion moins sécurisée, qui rend votre compte vulnérable. Vous pouvez désactiver l'accès pour ces applications (recommandé) ou l'activer si vous voulez les utiliser malgré les risques encourus. Google DÉACTIVE automatiquement ce paramètre s'il n'est pas utilisé. [En savoir plus](#)

Paramètre "Autoriser les applications moins sécurisées" activé



Pour ce faire je dois activer dans mes paramètres mails, « Autoriser les applications moins sécurisées ».

**Alert : proxy[6452] / host1 / 127.0.0.1**



**Jeremy DEBLAECKER** <jeremydeblaecker@gmail.com>

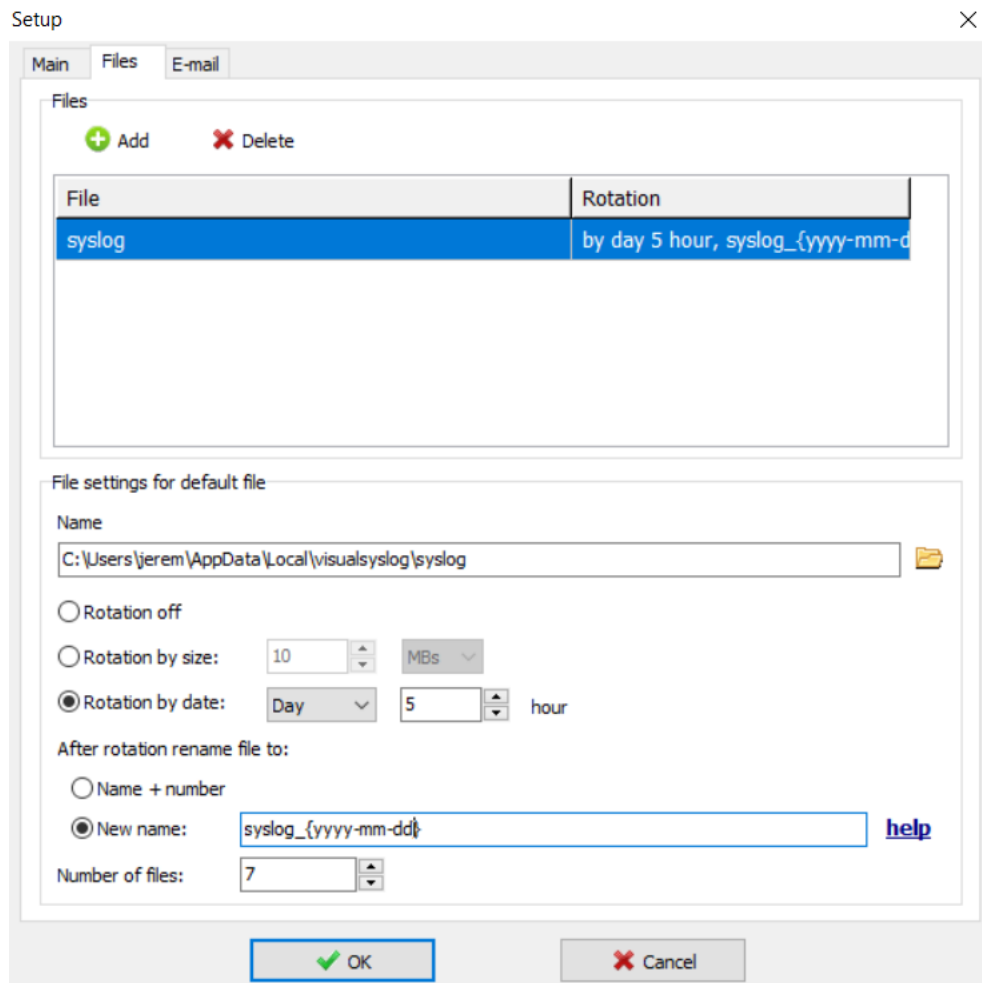
À jeremy.deblaecker ▾

Dec 1 13:56:04

Host or domain name not found

Ensuite je vérifie que j'ai bien reçu l'email de test : l'opération a fonctionné.

## Rotation des fichiers de log



Nous mettons en place maintenant des fichiers de Logs, il créera toutes les 5 heures tous les jours un fichier contenant des logs.

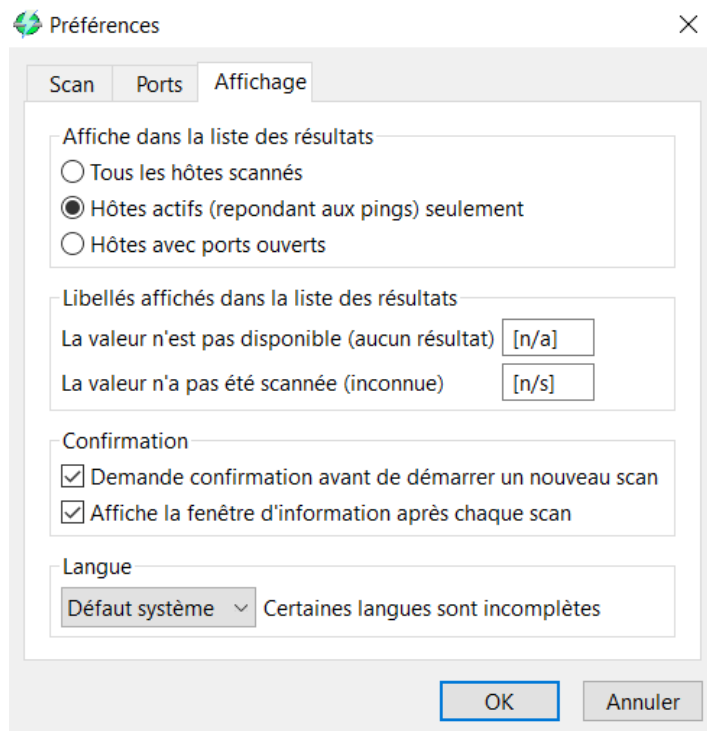
Sauvegarder ces logs est essentiel car requis par la loi, cependant ces logs peuvent être nombreuses c'est pour ça qu'il est également important de les filtrer avant de les envoyer par mail (par exemple, envoyer seulement les logs d'error).

Certains logs doivent être sauvegarder conformément à la Loi sur la Sécurité Quotidienne de 2001, mets ces logs doivent être anonymiser afin de protéger la vie privée des utilisateurs. Chaque entreprise est obligée de sauvegarder ces logs pendant un an afin que les autorités judiciaires puissent y accéder en cas de problème.

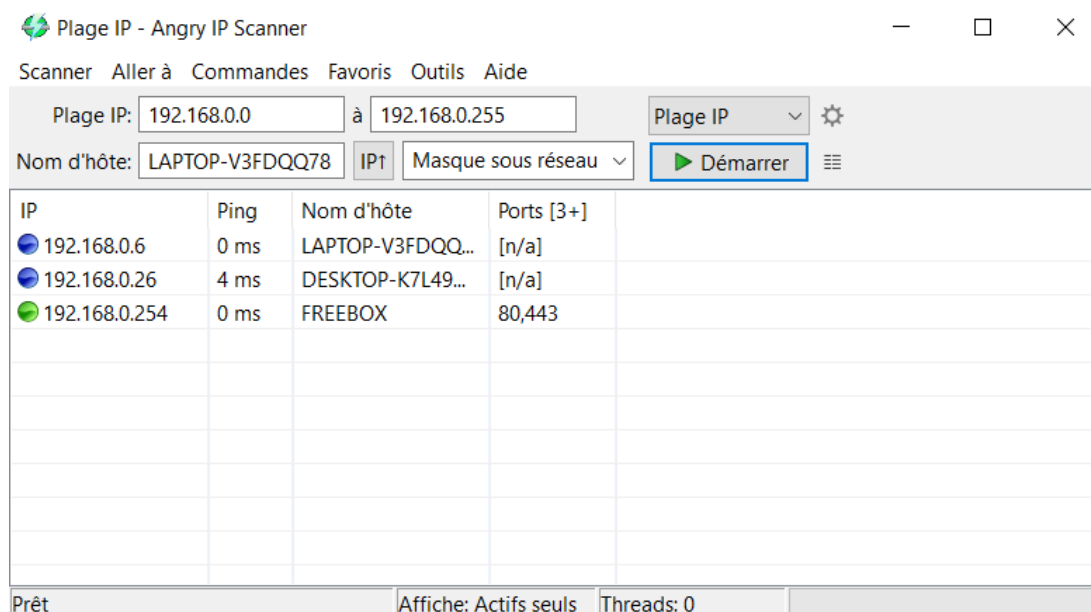
## Sixième TP : Découverte des Scanners

### Angry IP Scanner

Angry IP Scanner est un scanner d'adresse IP qui permet de récupérer les adresses IP d'un réseau.



Afin d'afficher seulement les IP actives, il suffit d'activer l'option hôte actif dans les paramètres.



Angry IP Scanner est très simple d'utilisation puisqu'il suffit juste de rentrer la plage IP qui nous intéresse pour voir les résultats.

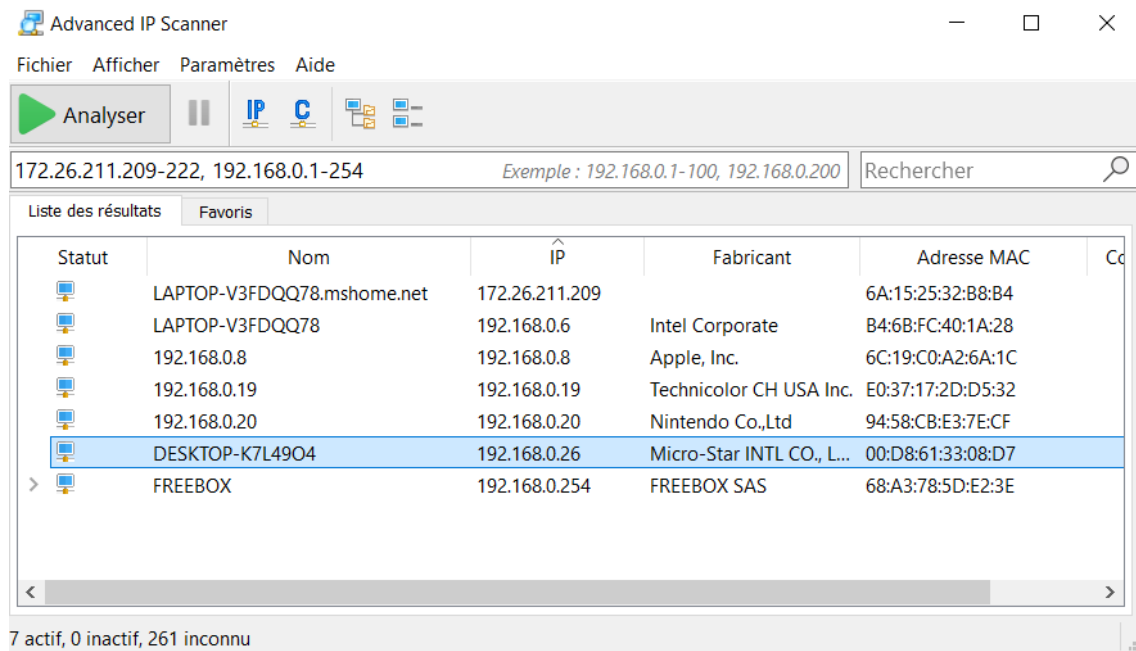
Comme vous pouvez le voir le scanner repère trois hôtes : mon ordinateur portable et fixe ainsi que ma Freebox.

Grâce au scanner, on peut connaître l'adresse IP, le nom d'hôte et le port de chacun des périphériques connectés au réseau.

Malheureusement, je remarque que certains hôtes n'apparaissent pas, par exemple, je sais qu'il y a des téléphones et des tablettes connectées à ce réseau qui ne sont pas prisent en compte par le scanner.



## Advanced IP Scanner



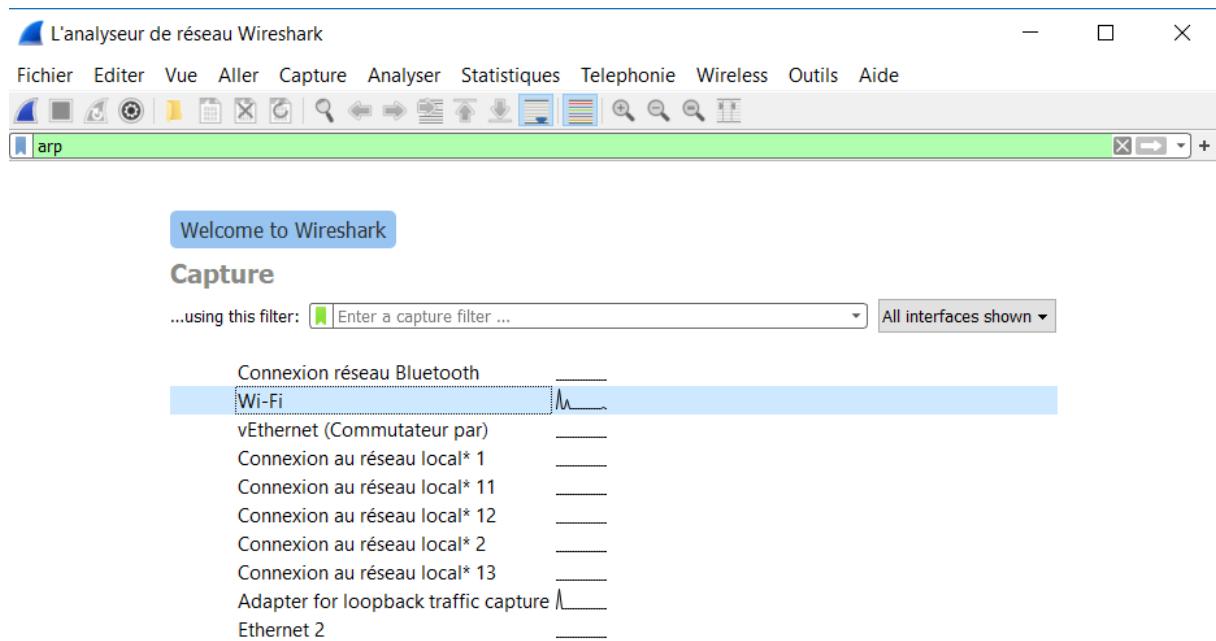
En utilisant Advanced IP Scanner je remarque, qu'il repère trois autres d'adresse IP, cependant il ne récupère pas le nom d'hôte de ces nouvelles IP. Je dois donc déduire à qui appartient ces IP : je remarque un produit Apple (surement mon téléphone), un produit Nintendo (une Switch) et la box Canal (fabricant technicolor CH USA).

Cependant malgré ces nouveaux hôtes, certains n'apparaissent toujours pas (téléphone/tablette).

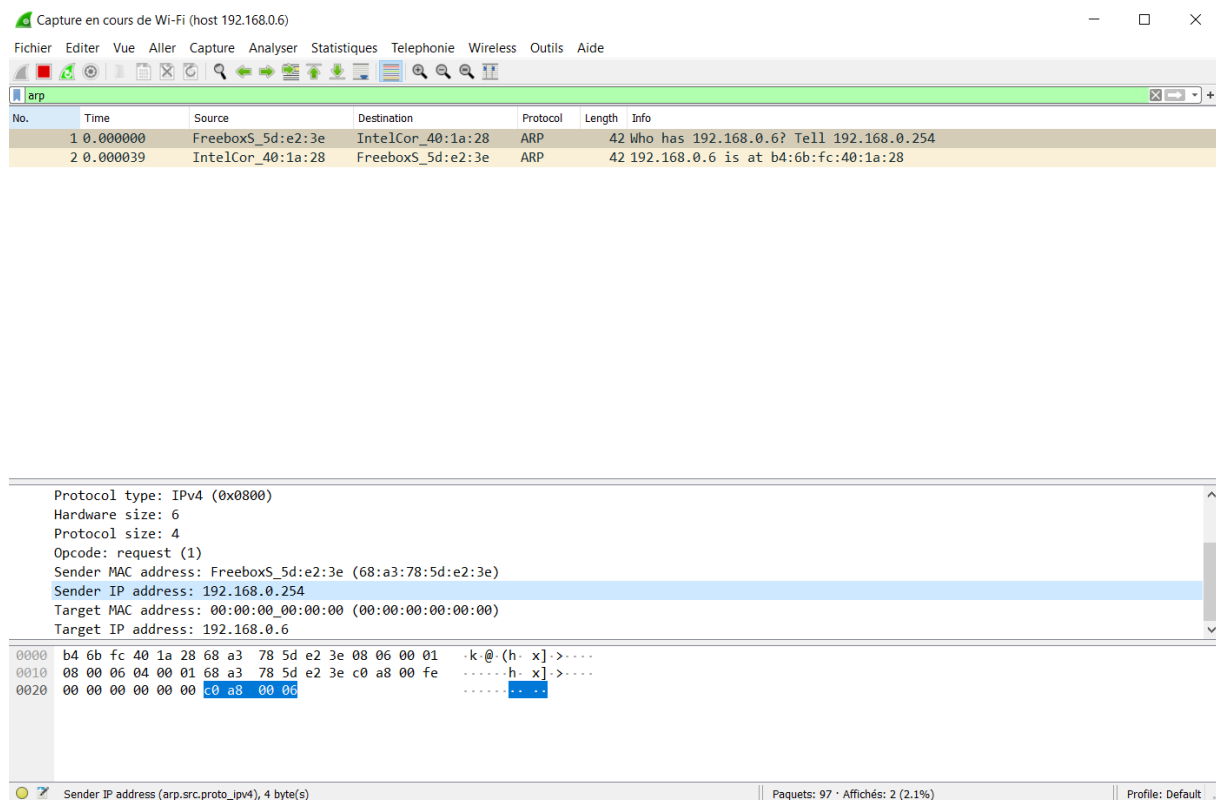
## Septième TP : Écoute et Analyse du réseau

### Étape #1





Sur Wireshark je capte les requêtes ARP sur le réseau entre mon PC et les périphériques.



Ici je vois bien que ma Freebox envoie une requête vers mon PC et il lui répond.

```
Interface : 192.168.0.6 --- 0x18
```

Adresse Internet	Adresse physique	Type
192.168.0.5	f8-d0-ac-19-72-db	dynamique
192.168.0.19	e0-37-17-2d-d5-32	dynamique
192.168.0.20	94-58-cb-e3-7e-cf	dynamique
192.168.0.26	00-d8-61-33-08-d7	dynamique
192.168.0.42	a4-d9-31-65-3b-ca	dynamique
192.168.0.254	68-a3-78-5d-e2-3e	dynamique
192.168.0.255	ff-ff-ff-ff-ff-ff	statique
224.0.0.22	01-00-5e-00-00-16	statique
224.0.0.251	01-00-5e-00-00-fb	statique
224.0.0.252	01-00-5e-00-00-fc	statique
239.255.255.250	01-00-5e-7f-ff-fa	statique
255.255.255.255	ff-ff-ff-ff-ff-ff	statique

En consultant le cache ARP de mon poste je vois bien que l'adresse ip qui m'a contacté est dans la liste des adresses IP.

## Étape #2

Capture en cours de Wi-Fi (host 192.168.0.6)

Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

No.	Time	Source	Destination	Protocol	Length	Info
159	9.606064	178.32.154.10	192.168.0.6	TCP	54	80 → 60845 [ACK] Seq=1 Ack=804 Win=30848 Len=0
160	9.606504	178.32.154.10	192.168.0.6	HTTP	649	HTTP/1.1 301 Moved Permanently (text/html)
161	9.618136	192.168.0.6	178.32.154.10	TLSv1.2	990	Application Data
162	9.647053	192.168.0.6	178.32.154.10	TCP	54	60845 → 80 [ACK] Seq=804 Ack=596 Win=65024 Len=0
163	9.709098	178.32.154.10	192.168.0.6	TCP	54	443 → 60843 [ACK] Seq=5942 Ack=2511 Win=34048 Len=0
164	9.877410	178.32.154.10	192.168.0.6	TLSv1.2	598	Application Data, Application Data
165	9.883610	192.168.0.6	178.32.154.10	HTTP	836	GET /etudiant?identifiant=HaVMY9kXNNvkhky5 HTTP/1.1
166	9.918968	192.168.0.6	178.32.154.10	TCP	54	60843 → 443 [ACK] Seq=2511 Ack=6486 Win=64256 Len=0
167	9.935576	178.32.154.10	192.168.0.6	HTTP	606	HTTP/1.1 301 Moved Permanently (text/html)
168	9.951100	192.168.0.6	178.32.154.10	TLSv1.2	969	Application Data
169	9.976061	192.168.0.6	178.32.154.10	TCP	54	60845 → 80 [ACK] Seq=1586 Ack=1148 Win=64512 Len=0
170	10.002530	178.32.154.10	192.168.0.6	TCP	54	443 → 60843 [ACK] Seq=6486 Ack=3426 Win=35968 Len=0
171	10.012050	178.32.154.10	192.168.0.6	TLSv1.2	1514	Application Data
172	10.012288	178.32.154.10	192.168.0.6	TLSv1.2	564	Application Data
173	10.012342	192.168.0.6	178.32.154.10	TCP	54	60843 → 443 [ACK] Seq=3426 Ack=8456 Win=65536 Len=0
174	10.356001	192.168.0.6	178.32.154.10	TLSv1.2	1000	Application Data

> Frame 165: 836 bytes on wire (6688 bits), 836 bytes captured (6688 bits) on interface \Device\NPF\_{DEE0F5E8-0FCD-4831-9ADD-A37325CA1D8D}, id 0  
 > Ethernet II, Src: IntelCor\_40:1a:28 (b4:6b:fc:40:1a:28), Dst: FreeboxS\_5d:e2:3e (68:a3:78:5d:e2:3e)  
 > Internet Protocol Version 4, Src: 192.168.0.6, Dst: 178.32.154.10  
 > Transmission Control Protocol, Src Port: 60845, Dst Port: 80, Seq: 804, Ack: 596, Len: 782  
 Source Port: 60845  
 Destination Port: 80

0020 9a 0a ed ad 00 50 e9 a2 44 5e e5 cf c9 fb 50 18 .....P..D^....P.  
 0030 00 fe 10 02 00 00 47 45 54 20 2f 65 74 75 64 69 .....GE T /etudi  
 0040 61 6e 74 3f 69 64 65 6e 74 69 66 69 61 6e 74 3d ant?iden tifiant=  
 0050 48 61 56 4e 59 39 6b 58 4e 4e 76 6b 68 6b 79 35 HaVMY9kX NNvkhky5  
 0060 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a HTTP/1. 1 -Host:  
 0070 20 68 70 31 39 79 2e 79 6e 6f 76 2e 63 6f 6d 0d hp19y.y nov.com

Depuis l'extranet d'Ynov je me connecte à mon compte, wireshark capte cette connexion. En effet mon ip (192.168.0.6) se connecte à ynov (178.32.154.10). On voit dans les informations de cette connexion que je fourni mes identifiants étudiants grâce au protocole HTTP.

```
C:\Users\jerem>ping hp19y.ynov.com

Envoi d'une requête 'ping' sur reverseproxy2.ynov.com [178.32.154.10] avec 32 octets de données :
Réponse de 178.32.154.10 : octets=32 temps=44 ms TTL=56
Réponse de 178.32.154.10 : octets=32 temps=43 ms TTL=56
Réponse de 178.32.154.10 : octets=32 temps=43 ms TTL=56
Réponse de 178.32.154.10 : octets=32 temps=44 ms TTL=56

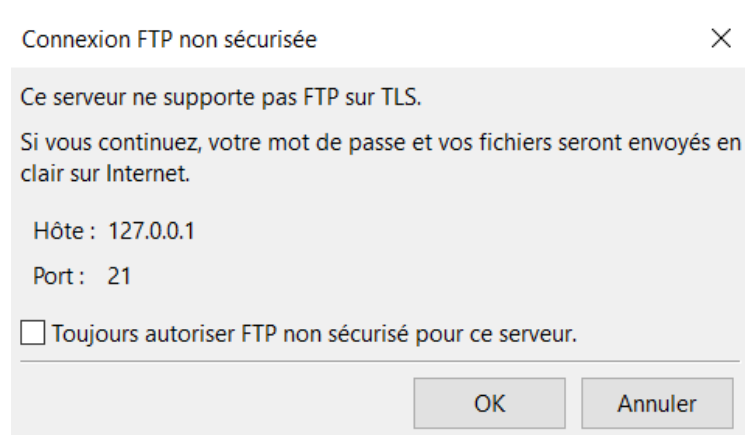
Statistiques Ping pour 178.32.154.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 43ms, Maximum = 44ms, Moyenne = 43ms
```

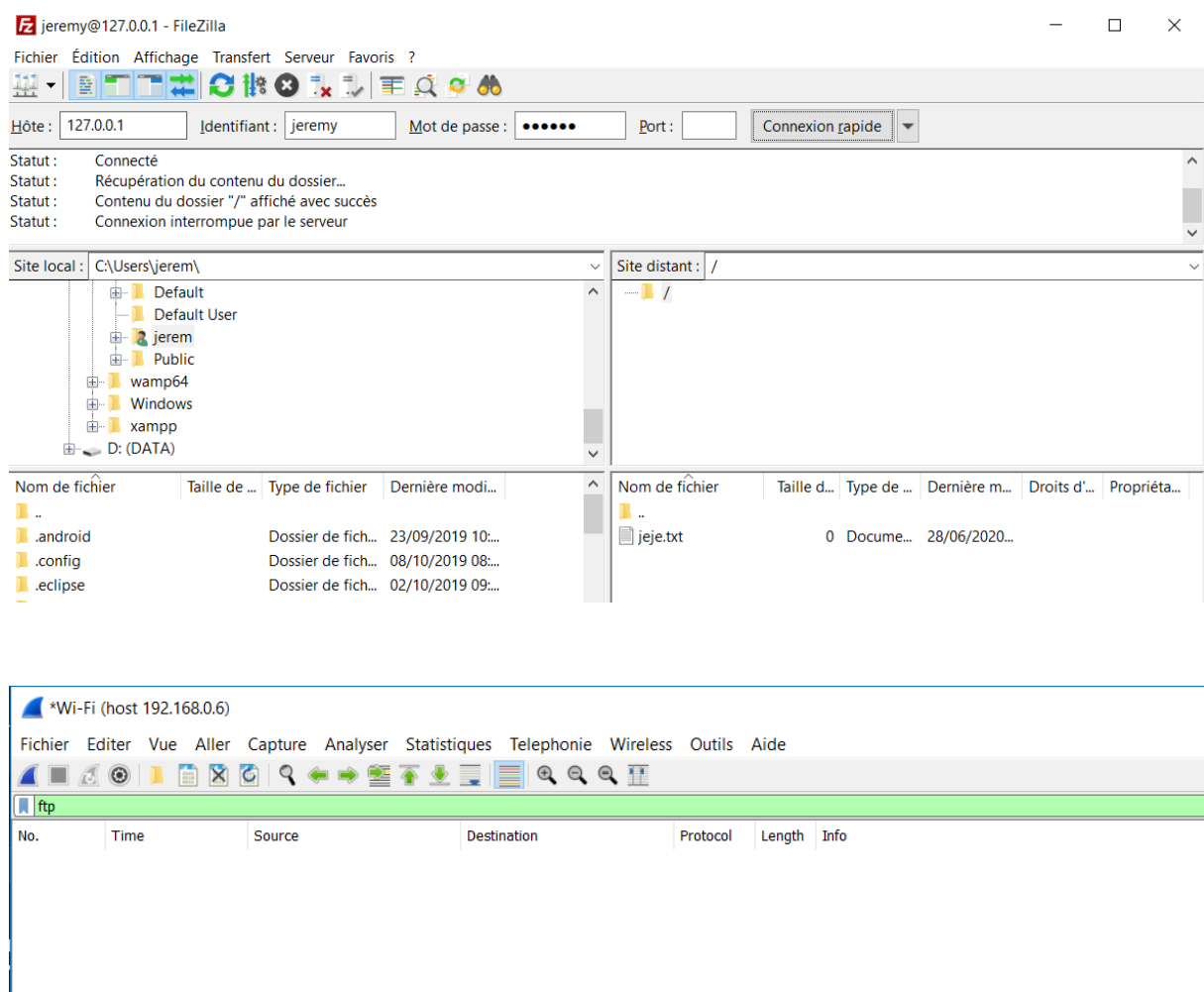
J'essaye de pinger Ynov depuis mon terminal afin de vérifier qu'il s'agit bien de son adresse IP, je remarque que c'est bien l'adresse IP d'Ynov.

Le numéro de séquence est choisi aléatoirement par les machines quand elles communiquent entre elles, en effet la création d'un numéro de séquence permet d'identifier la session. La création d'un numéro de séquence permet d'éviter les piratages.

## Étape #3

J'ai essayé de créer une communication entre le serveur FTP et mon hôte mais malheureusement je n'ai pas réussi à créer de communication entre les deux.





J'ai pense cependant avoir paramétré correctement FileZilla puisque j'arrive à récupérer le fichier que j'avais préalablement créé dans mes fichiers en utilisant le compte que j'avais créé.