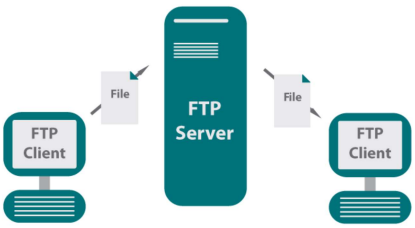
BTS SIO SISR
Protocole FTP (et FTPS)



Le protocole FTP (*File Transfer Protocol* ou protocole de transfert de fichier) est un protocole de communication destiné au partage de fichiers sur un réseau. Il permet principalement de téléverser (*upload*) des fichiers vers un autre ordinateur ou d'en télécharger (*download*).

On utilise souvent le protocole FTP pour « envoyer » ses pages (HTML, PHP, CSS, etc.) sur le serveur web (par exemple Apache) hébergé chez un prestataire pour qu'elles soient disponibles pour les internautes.

Remarque importante : les données circulent en clair. Pour sécuriser (c'est-à-dire assurer au minimum la confidentialité) on peut mettre en place du chiffrement SSL/TLS avec un certificat (confidentialité, intégrité et authentification 😉). Le protocole se dénommera alors FTPS.

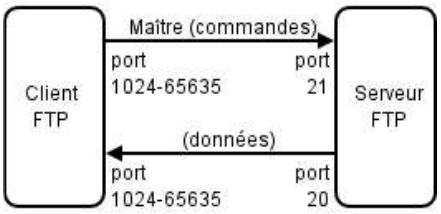
FTP fonctionne avec le modèle client-serveur : le client se connecte au serveur et envoie des requêtes, le serveur répond ensuite aux requêtes. En pratique, le serveur est un ordinateur sur lequel fonctionne un logiciel lui-même appelé serveur FTP, qui rend disponible une arborescence de fichiers (un dossier par exemple) aux clients qui s'y connectent. Et pour accéder à un serveur FTP, on utilise un logiciel client FTP (possédant une interface graphique ou en ligne de commande).

Par convention, deux ports sont attribués (*well known ports*) pour les connexions FTP : le port 21 pour les commandes et le port 20 pour les données.

Types de connexions

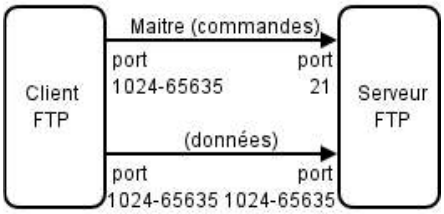
FTP peut s'utiliser de deux façons différentes :

Mode actif



En mode **actif**, c'est le client FTP qui détermine le port de connexion à utiliser pour permettre le transfert des données. Ainsi, pour que l'échange des données puisse se faire, le serveur FTP initialisera la connexion de son port de données (port 20) vers le port spécifié par le client. Le client devra alors configurer son pare-feu pour autoriser les nouvelles connexions entrantes afin que l'échange des données se fasse.

Mode passif



En mode **passif**, le serveur FTP détermine lui-même le port de connexion à utiliser pour permettre le transfert des données (data connexion) et le communique au client. En cas de présence d'un pare-feu devant le serveur, celui-ci devra être configuré pour autoriser la connexion de données. L'avantage de ce mode est que le serveur FTP n'initialise aucune connexion. Dans les nouvelles implémentations, le client initialise et communique directement par le port 21 du serveur ; cela permet de simplifier la configuration du pare-feu.

Commandes

Le client envoie une commande sous la forme d'une ligne de texte qui sera exécutée par le serveur.

Commandes principales :

- `pwd` (pour savoir dans quel dossier on se situe)
- `ls` (pour lister le contenu du dossier courant)
- `cd` (pour changer de dossier)
- `get` (pour télécharger un fichier)
- `send` (pour téléverser un fichier)
- `close` (pour terminer la connexion FTP)
- `quit` (pour quitter le client FTP)

Procédure de mise en place d'un service FTP

Objectif : configurer le service FTP sur un serveur web afin que les membres du groupe webmaster puisse gérer les fichiers du serveur web (situés dans le dossier /var/www/).

Etapes :

1. Démarrer une machine Linux Debian (configurée sur le réseau de la classe, donc avec un accès INTERNET, et possédant déjà la fonctionnalité de serveur web avec apache), mettre à jour la liste des paquets et installer le paquet proftpd (→ la machine Linux Debian deviendra désormais un « serveur FTP » en plus d'un serveur web 😉)

2. Récupérer l'adresse IP du serveur et tester (depuis un navigateur web) l'affichage du site web déjà configurée (par exemple Netflix ou HomeDecoration).

3. Dans le répertoire /var/www, créer un dossier « netflix » et un dossier « homedecor ». Créer un fichier « index.html » à l'intérieur de chacun, avec le contenu suivant : « <html><body>Site en construction</body></html>.

4. On souhaite confier la gestion du site web Netflix à une équipe de webmaster. Pour l'instant, seuls les salariés Alexis et Esteban sont habilités à intervenir sur le site web. Leur collègue Léa attend la fin d'une formation.

   Créer l'utilisateur « alexis » (en minuscules), l'utilisateur esteban et l'utilisateur « lea » (mot de passe identique au nom). Créer un nouveau groupe « webmaster ». Ajouter les utilisateurs « alexis » et « esteban » au groupe « webmaster ».

   Remarque : l'utilisateur créé sur Linux n'est pas qu'un simple utilisateur de FTP. En effet, il pourra avoir accès au système (en local, ou via SSH éventuellement) et par conséquent réaliser d'autres tâches (créer d'autres utilisateurs, modifier les fichiers du système, etc. -bien évidemment, s'il possède des droits suffisants-). Ce qui peut poser des problèmes de sécurité. Si on veut créer un utilisateur sans « droit » sur le système (donc sans shell afin de ne pas pouvoir saisir de commandes), il faut suivre cette procédure :

   `echo "/bin/false" >> /etc/shells` ← On ajoute « Aucun shell » à la liste des shell disponibles 😊
   `adduser nomUtilisateur --shell /bin/false` ← Pour ajouter un utilisateur sans shell

5. Actuellement, le dossier du serveur web (« /var/www/ ») possède les droits suivants (via la commande `ls -l /var/www`) :
   `r w x r _ x r _ x  root  root  netflix`
   `r w x r _ x r _ x  root  root  homedecor`

   Ce qui signifie que l'utilisateur propriétaire du dossier « netflix » et du dossier « homedecor » est « root » (il peut lire, écrire et exécuter) et le groupe propriétaire est « root » (même droits mais sans l'écriture).

   Modifier les droits sur les dossiers du serveur web (et tous les sous-dossiers et fichiers à l'intérieur → on appelle ceci la récursivité) pour que le groupe webmaster soit propriétaire à la place du groupe « root ». C'est important car c'est le groupe « webmaster » qui sera chargé de gérer le serveur web et donc les fichiers du ou des sites web !

6. Le contenu du dossier « netflix » (par exemple ici le fichier « index.html ») présente les droits suivants (utiliser la commande `ls -l /var/www/netflix`) :
   `r w _ r _ _ r _ _` `root  webmaster  index.html`
   Ce qui signifie que l'utilisateur propriétaire « root » peut lire et modifier le fichier et le nouveau groupe propriétaire « webmaster » ne peut que lire le fichier (pas le modifier).

   Modifier également les droits pour que le groupe propriétaire (« webmaster ») puisse avoir également le droit d'écrire (indispensable pour que le webmaster puisse modifier le site web) et exécuter. Faire la même chose pour le dossier « homedecor ».

7. Editer le fichier de configuration /etc/proftpd/proftpd.conf

8. Modifier la ligne « ServerName » pour donner un nom plus convivial au serveur FTP (par exemple : ServerName "netflix"). Ce nom sera affiché lors de la connexion au service FTP.

9. Laisser la ligne « MaxInstances 30 » afin de n'autoriser que 30 connexions simultanées et éviter les attaques DDoS.

10. Laisser le port par défaut 21 (ou changer le numéro du port pour dissimuler le service FTP)

11. Modifier la ligne « Umask » pour avoir afin d'enlever le droit d'écriture aux autres utilisateurs sur tous les fichiers nouvellement créés via FTP :
```
Umask 002
```

12. Laisser pour le moment le mode actif en laissant le hastag devant la ligne « # PassivePorts 49152 65534 ». Donc notre serveur FTP sera en mode actif, ce qui signifie qu'il faudra paramétrer le pare-feu local du poste client.

13. On souhaite restreindre tous les utilisateurs FTP à leur dossier personnel (afin qu'ils ne puissent pas naviguer n'importe où sur le système), sauf le groupe webmaster qui pourra aller sur le dossier du serveur web. Ajouter les lignes suivantes dans le fichier de configuration :
```
DefaultRoot ~ !webmaster
```

14. On souhaite que les membres du groupe webmaster n'accède qu'aux fichiers du serveur web. Pour ce faire, ajouter cette ligne également :
```
DefaultRoot /var/www webmaster
```

    Ainsi, dès qu'un webmaster se connectera en FTP, il ne verra qu'un « / » qui pointera vers « /var/www/ ». C'est très sécurisant de faire ceci. On appelle ceci « chrooter » 😉

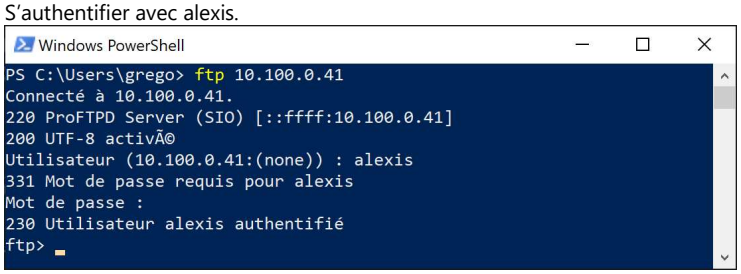
15. Pour l'instant, « alexis » et « esteban », les 2 webmaster, peuvent accéder aux fichiers du serveur web (« /var/www »). Toutefois, le site web en construction (contenu dans le dossier « homedecor ») ne doit être modifié que par « alexis ». Ajouter les lignes suivantes à la fin du fichier de configuration « proftpd.conf » :
```
<Directory /var/www/homedecor>
  Umask 002
  AllowOverwrite on
  #Droits pour la connexion FTP
  <Limit LOGIN>
    AllowUser alexis
    #Si on souhaite accorder les droits au groupe webmaster, on écrit : AllowGroup webmaster
    DenyAll
  </Limit>
  #Droits pour l'exécution de commandes FTP
  <Limit ALL>
    AllowUser alexis
    DenyAll
  </Limit>
</Directory>
```

16. Redémarrer le service proftpd

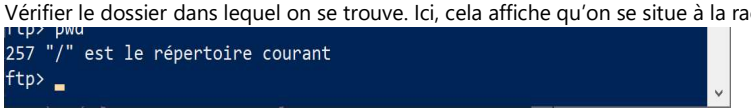
Remarque : si le redémarrage du service génère une erreur, relire le fichier de configuration à la recherche d'erreurs de syntaxe 😉.

Test d'accès au service FTP avec Powershell :

1. Exécuter PowerShell et saisir la commande de connexion au service FTP (regarder où on se situe avant de lancer FTP, ici on est sur P:\). S'authentifier avec alexis.

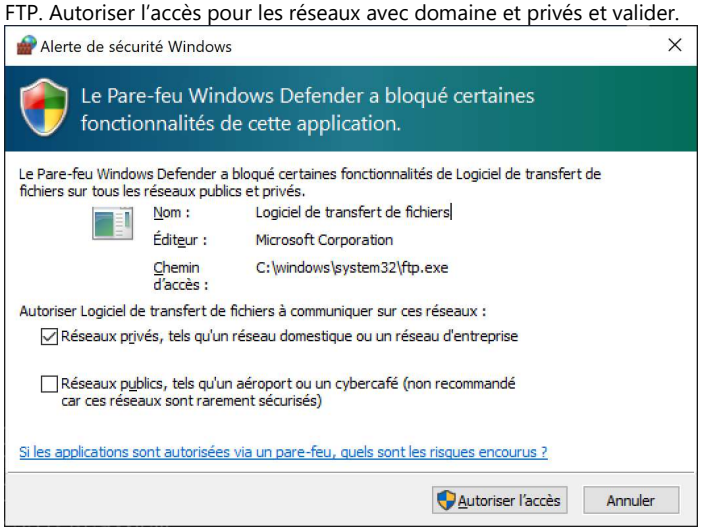


2. Vérifier le dossier dans lequel on se trouve. Ici, cela affiche qu'on se situe à la racine « / ». Mais en réalité, on se situe dans « /var/www ».

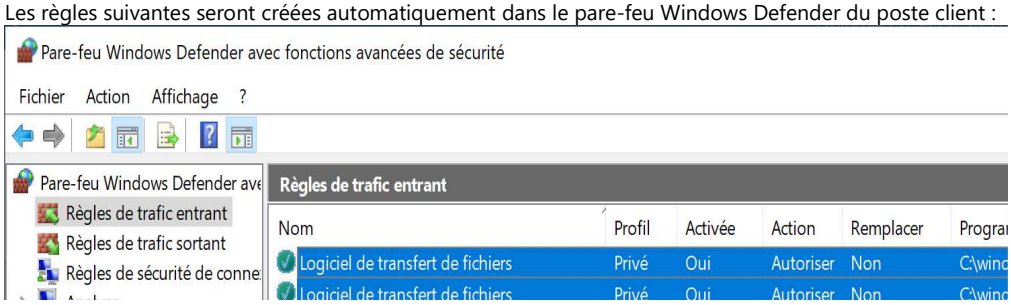


3. Afficher le contenu du dossier avec la commande « ls »

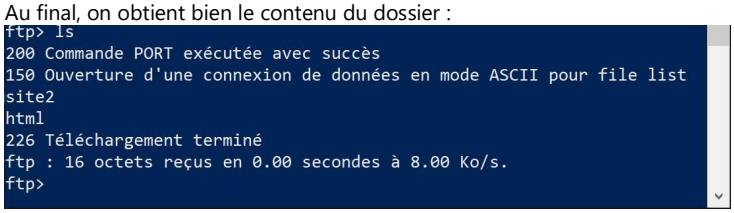
Attention, une alerte du pare-feu va apparaitre pour autoriser les flux car on est en mode actif et c'est la première fois qu'on utilise le client FTP. Autoriser l'accès pour les réseaux avec domaine et privés et valider.



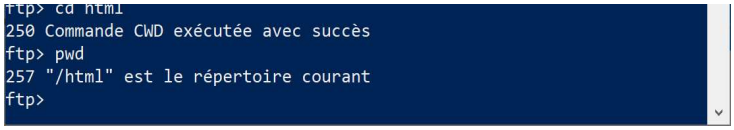
Les règles suivantes seront créées automatiquement dans le pare-feu Windows Defender du poste client :



Au final, on obtient bien le contenu du dossier :



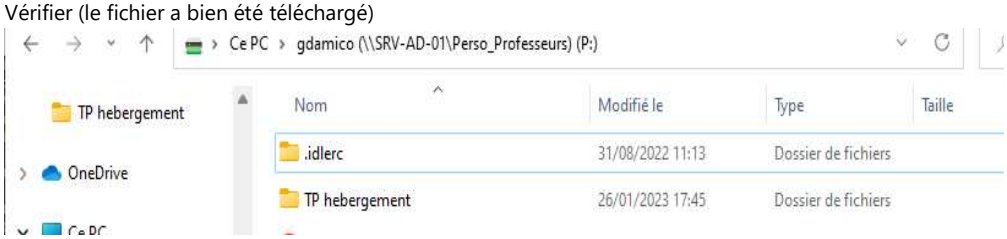
4. Aller dans le sous-dossier « netflix » et vérifier qu'on est dans le bon dossier (attention, ici c'est marqué « html » mais vous cela doit être écrit « netflix ».



5. Télécharger le fichier (il s'enregistrera sur le répertoire où on se situait, sur PowerShell, avant de lancer la commande FTP -dans l'exemple ici, c'est le répertoire personnel P:\-)

```
ftp> get index.html
200 Commande PORT exécutée avec succès
150 Opening ASCII mode data connection for index.html (10709 bytes)
226 Téléchargement terminé
ftp : 11077 octets reçus en 0.00 secondes à 11077.00 Ko/s.
ftp>
```

6. Vérifier (le fichier a bien été téléchargé)



7. Modifier le contenu du fichier « index.html » (c'est plus simple sur un Windows 😉) en simulant une mise à jour de la page web, par exemple en vidant tout le contenu et en ajoutant le contenu suivant :
   <html>
   <body>
   Site web mis à jour par le webmaster Alexis
   </body>
   </html>

8. Téléverser le fichier modifié (« index.html ») sur le serveur web via FTP (si cela ne fonctionne pas, et qu'on n'a pas les droits sur le dossier et donc que les étapes 3 et 4 n'ont pas été respectées)

```
ftp> send index.html
200 Commande PORT exécutée avec succès
150 Ouverture d'une connexion de données en mode ASCII pour index.html
226 Téléchargement terminé
ftp : 11077 octets envoyés en 0.03 secondes à 325.79 Ko/s.
ftp>
```

9. Fermer la connexion et quitter FTP

```
ftp> close
221 Au revoir.
ftp> quit
PS C:\Users\grego>
```

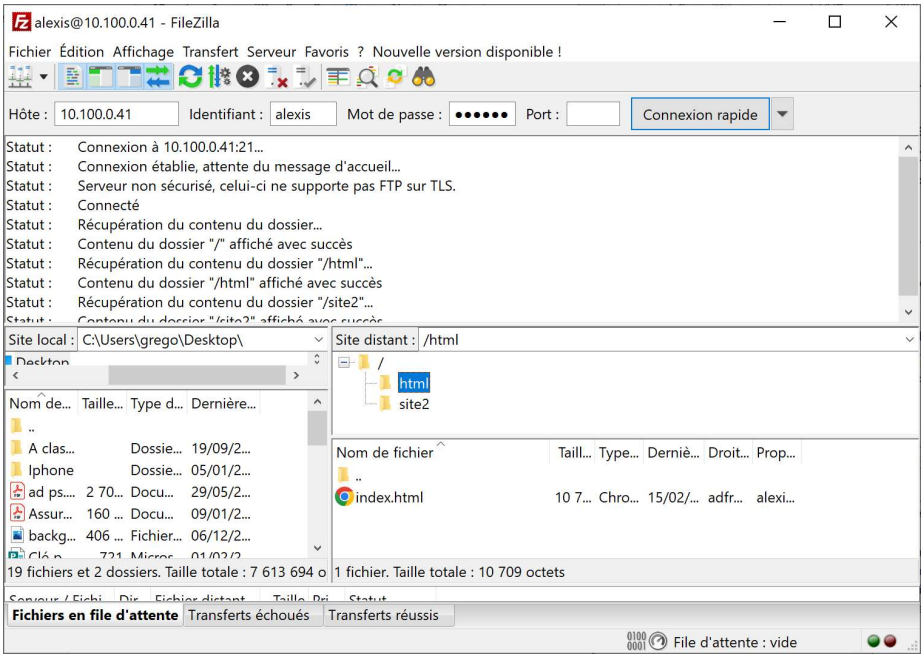
10. Tester l'accès au site web avec un navigateur (normalement, la nouvelle page devrait s'afficher 😉)

11. Recommencer la connexion FTP avec l'utilisateur « lea ». Normalement, elle ne peut pas interagir sur le dossier du serveur web (/var/www/) ; elle a accès uniquement à son dossier personnel. Tester ensuite avec « esteban ». Il est « enfermé » dans le dossier « /var/www/ » et peut donc accéder au dossier « netflix » mais pas au dossier « homedecor » car on a mis une restriction.

Si on ne souhaite pas utiliser la version ligne de commandes, on peut utiliser un client FTP graphique avec le logiciel gratuit FileZilla. Cette méthode est obligatoire pour se connecter sur en FTPS (sécurisé).

C'est un peu plus simple à utiliser qu'en ligne de commande.

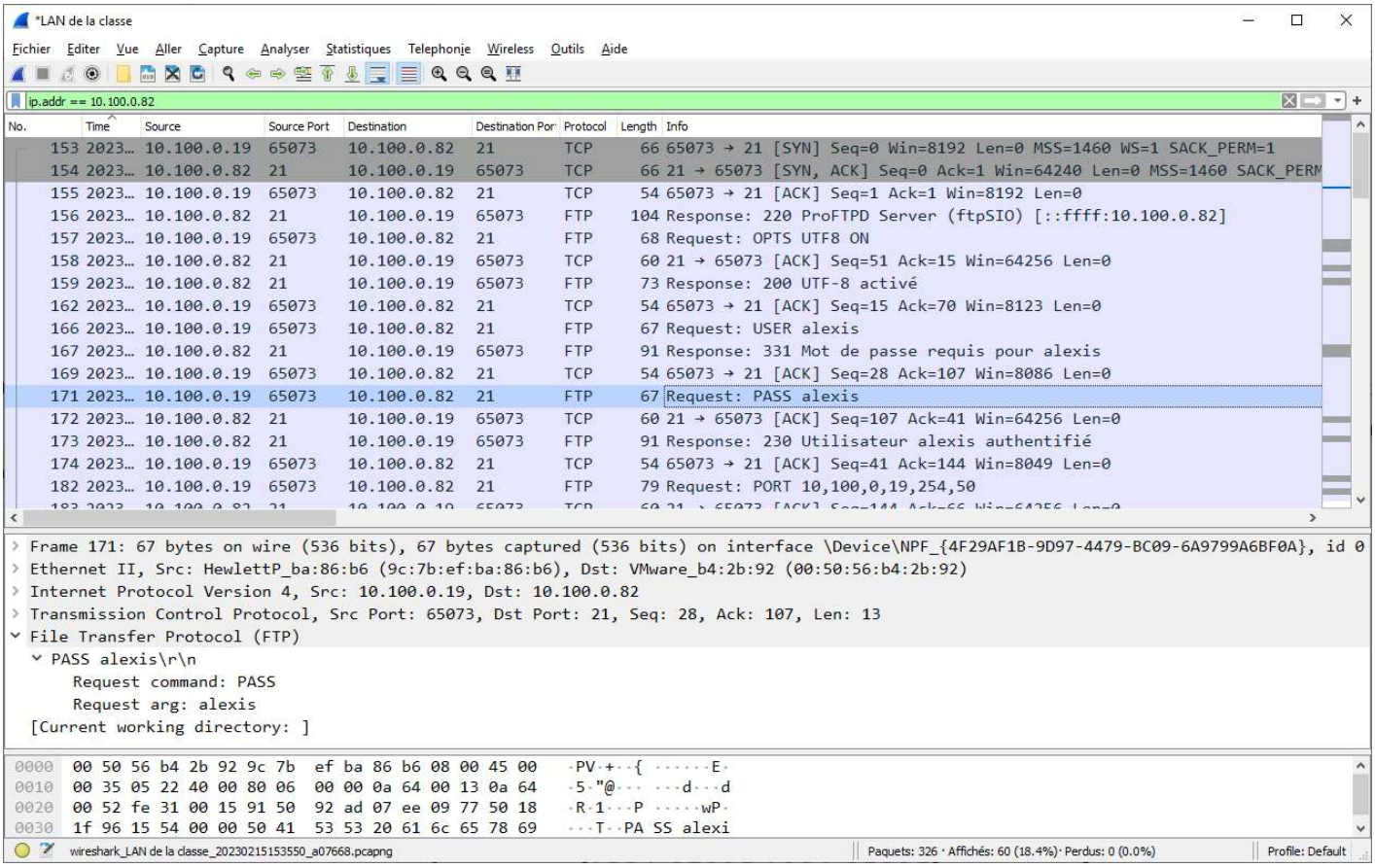
Dans notre exemple ici, on voit bien qu'Alexis a accès au serveur web (/var/www) et notamment les dossiers « html » et « site2 » (vous ça sera affiché « netflix » et « homedecor ». Mais ces dossiers s'affichent directement sous la racine « / » car on a enfermé « alexis » dans « /var/www » avec l'option « DefaultRoot » 😉.



Travail supplémentaire à faire :

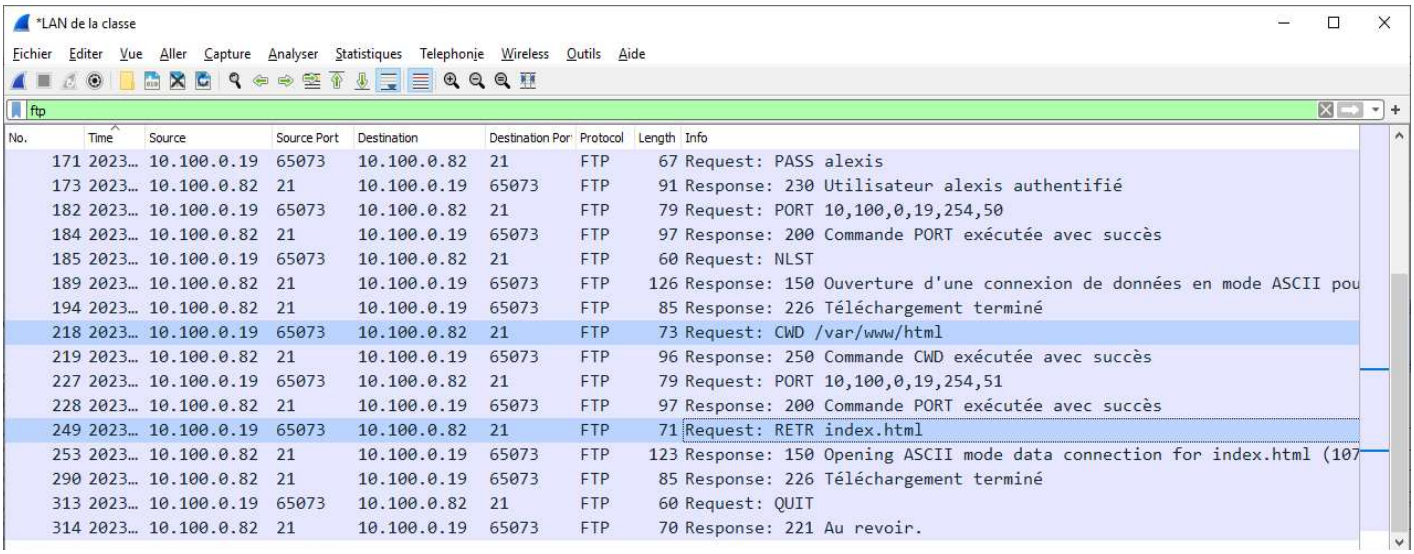
Sur votre PC Windows 10 (sur lequel est installé le logiciel client Filezilla ou Powershell pour se connecter en ligne de commande), lancer la capture Wireshark et se connecter au serveur FTP. Prouver que les données transitent en clair (absente de confidentialité, donc problème de sécurité.

Normalement, on doit avoir ce résultat avec Wireshark :



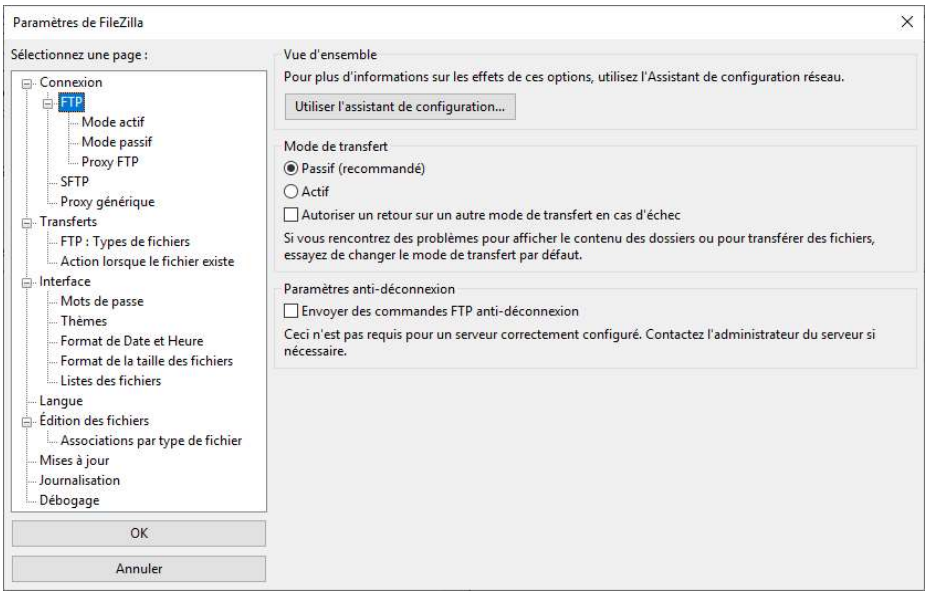
On a filtré sur l'IP du serveur FTP (ici, l'IP du serveur est désormais 10.100.0.82). Ainsi, on récupère toutes les trames (TCP et FTP) générées pour le service FTP. On aurait pu aussi filtrer uniquement sur le protocole FTP, mais on n'aurait pas eu les échanges (handshake, ack…) complets.

Lorsqu'on regarde les flux TCP, on peut voir que les données circulent en clair (le mot de passe de l'utilisateur « alexis » par exemple, ou encore les commandes pour changer de dossier ou télécharger un fichier) :



La machine cliente (10.100.0.19) émet un flux en sortie (donc autorisé par défaut par le pare-feu local Windows Defender), depuis le port 65073, vers le serveur FTP (10.100.0.82) sur le port 21. C'est une demande de synchronisation (SYN). La « poignée de main » (handshake TCP) continue. Ensuite, les échanges FTP se font.

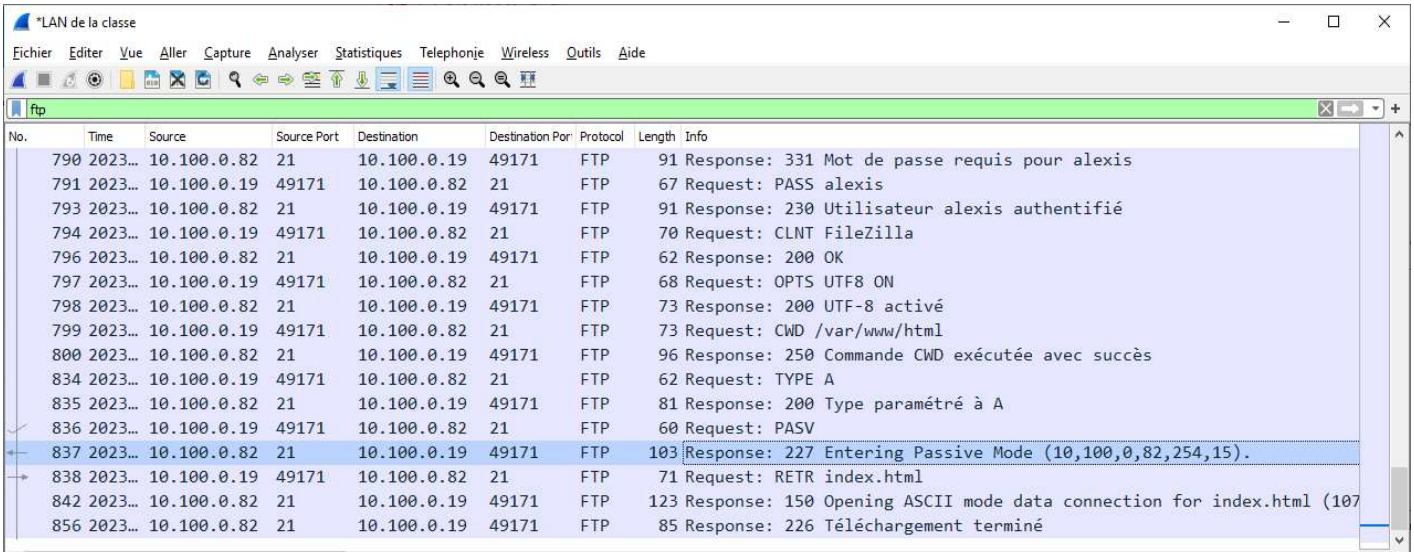
Pour forcer le mode passif (donc pour éviter de toucher au pare-feu local du poste client Windows), on peut utiliser le logiciel FileZilla, aller dans le menu Editer, Paramètres, puis cliquer sur FTP et décocher la case « Autoriser un retour sur un autre mode » (en vérifiant bien que le mode passif est sélectionné).



Il faut également modifier le fichier de configuration « proftpd.conf » est décommenter la ligne « # PassivePorts … », enregistrer puis redémarrer le service.

Pour réaliser un test réaliser, il faut supprimer ou désactiver les autorisations FTP en flux entrants sur le pare-feu local du client Windows :

Ensuite, en re-testant, on s'aperçoit que les flux passent correctement alors qu'il n'y a plus aucune autorisation explicite sur le pare-feu Windows. Dans la capture de trames, on peut voir qu'on est en mode passif « Entering Passive Mode » et que les flux passent correctement « Téléchargement terminé ».



Procédure de mise en place d'un service FTPS (FTP + SSL/TLS)

Objectif : actuellement, le service FTP proposé n'est pas en mesure d'assurer la confidentialité des données (les données circulent en clair sur le réseau, on peut donc capturer -avec Wireshark- les identifiants, les fichiers, etc. On souhaite donc mettre une couche de chiffrement (avec SSL/TLS) pour transformer notre service en FTPS.
Une autre façon de faire serait d'utiliser le protocole SFTP (qui utilise en réalité SSH 😉). Ceci nécessite d'installer SSH en plus…

Etapes :

1. Ajouter le paquet proftpd-mod-crypto.

2. Créer un nouveau dossier nommé « ssl » situé directement à la racine « / » :

3. Créer un nouveau certificat SSL (avec l'outil openssl) nommé « cert.pem », avec sa clé privée nommé « key.pem », et les stocker dans le dossier créé précédemment (« /ssl/ ») :

4. Afin d'activer le module SSL/TLS et lui indiquer où trouver le certificat à présenter aux clients et quelle clé de déchiffrement utiliser, ajouter les lignes suivantes à la fin du fichier de configuration « proftpd.conf » :

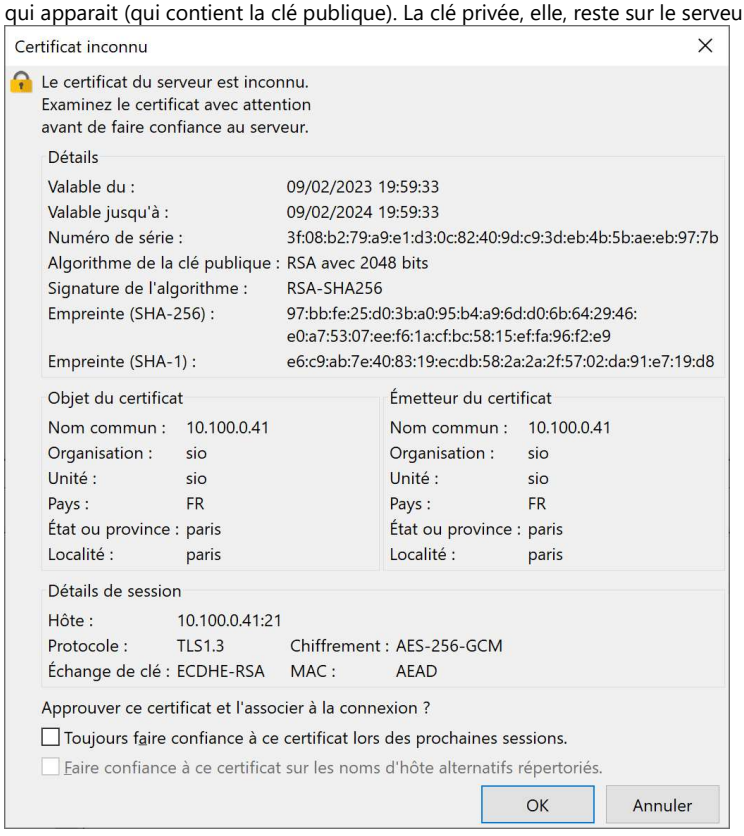
```
LoadModule mod_tls.c
<IfModule mod_tls.c>
  TLSEngine on
  TLSLog /var/log/proftpd/tls.log
  TLSProtocol SSLv23 TLSv1 TLSv1.1 TLSv1.2
  TLSRSACertificateFile /ssl/cert.pem
  TLSRSACertificateKeyFile /ssl/key.pem
  TLSVerifyClient off
  TLSRequired on
</IfModule>
```

5. Redémarrer le service proftpd

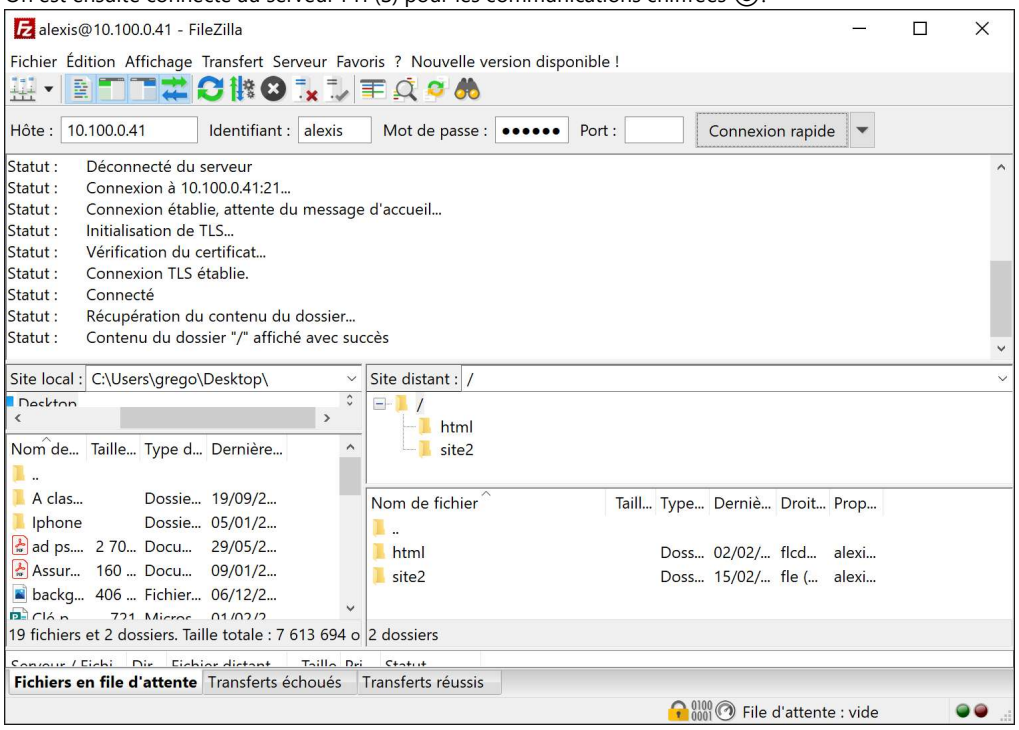
Test d'accès au service FTPS :

1. Exécuter le logiciel client FileZilla et lancer une nouvelle connexion vers le serveur FTP(S) avec l'utilisateur « alexis ».

2. Comme on a mis « TLSRequired on » dans le fichier de configuration, on est obligé de passer par FTPS et non FTP. On a donc le certificat qui apparait (qui contient la clé publique). La clé privée, elle, reste sur le serveur pour déchiffrer les communications.



3. On est ensuite connecté au serveur FTP(S) pour les communications chiffrées 😊.



Travail supplémentaire à faire :

Sur votre PC Windows 10 (sur lequel est installé le logiciel client Filezilla), lancer la capture Wireshark et se connecter au serveur FTPS. Prouver que les données sont désormais chiffrées.

Normalement, on doit voir les flux chiffrés avec TLS (ainsi, plus de mot de passe en clair 😉) :