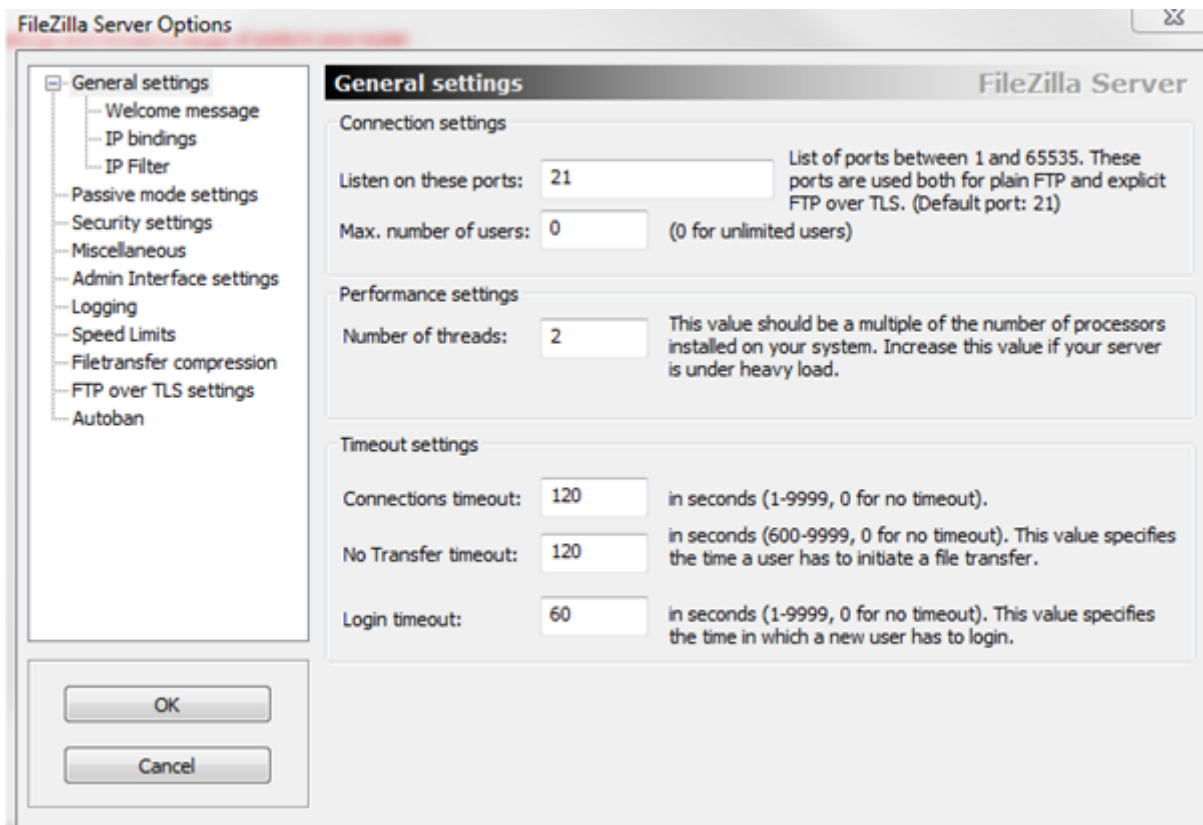
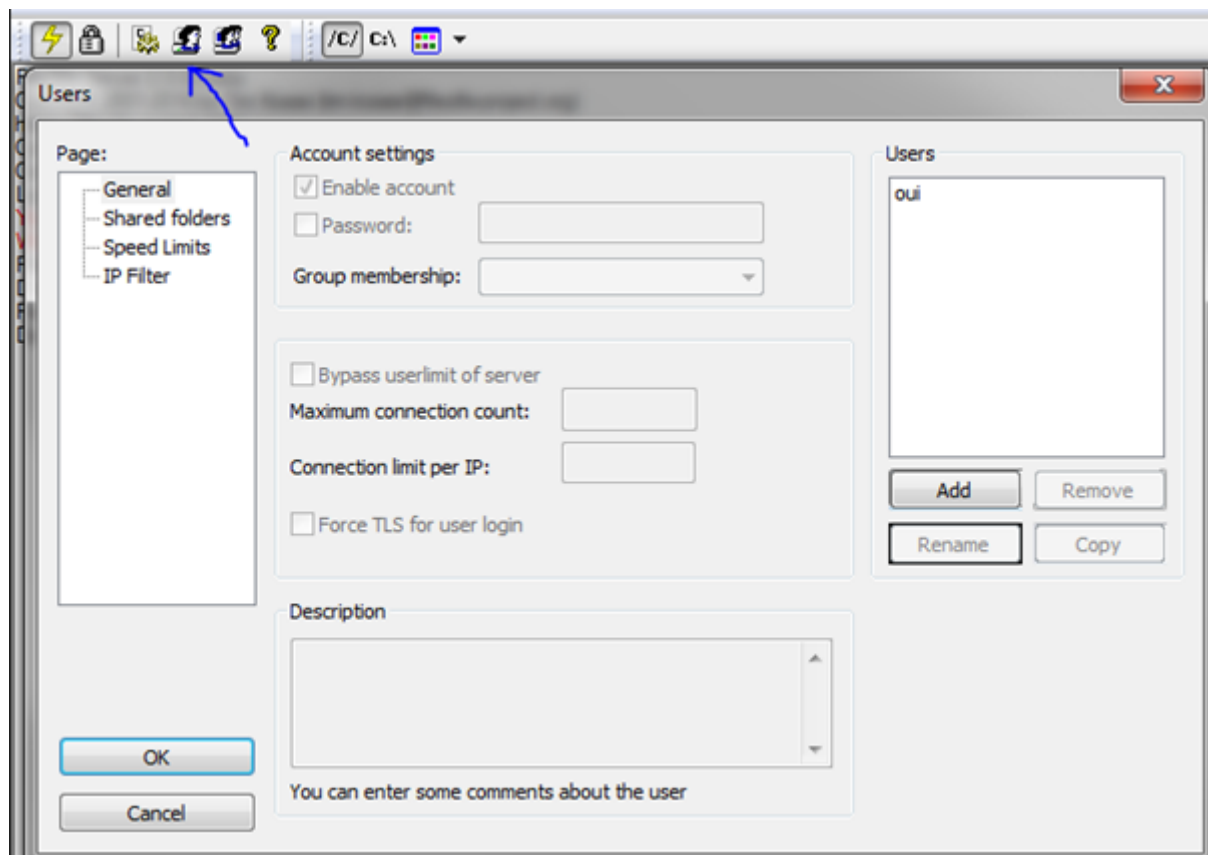


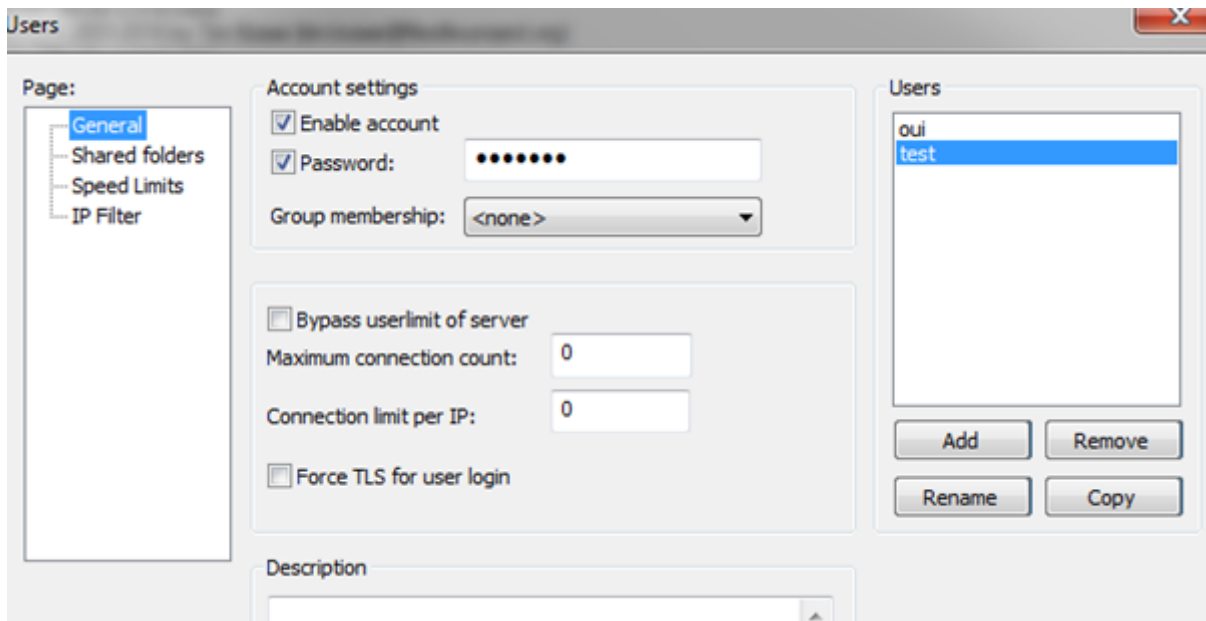
Serveur FTP non sécurisé



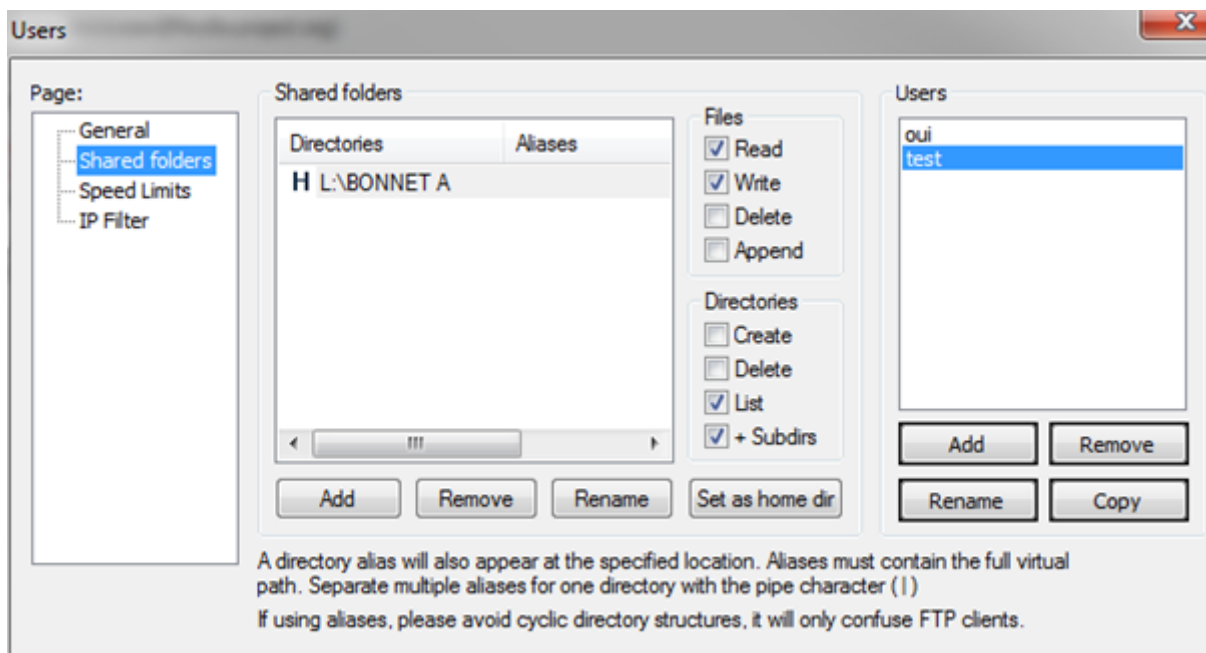
Ici on peut voir les paramètres du serveur FileZilla. Le port est par défaut à 21 et le nombre d'utilisateurs à 0 (ce qui correspond à illimité).



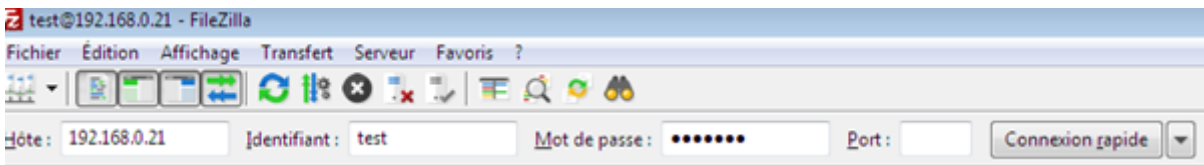
En cliquant sur cette icône, on a accès à la liste des utilisateurs. Nous allons en créer un en cliquant sur Add sur le côté droit. On définit un nom d'utilisateur et un mot de passe.



Une fois le nom de l'utilisateur et mot de passe définis, on clique sur « Shares folders ». Ce sont les dossiers partagés entre le serveur et l'utilisateur concerné.

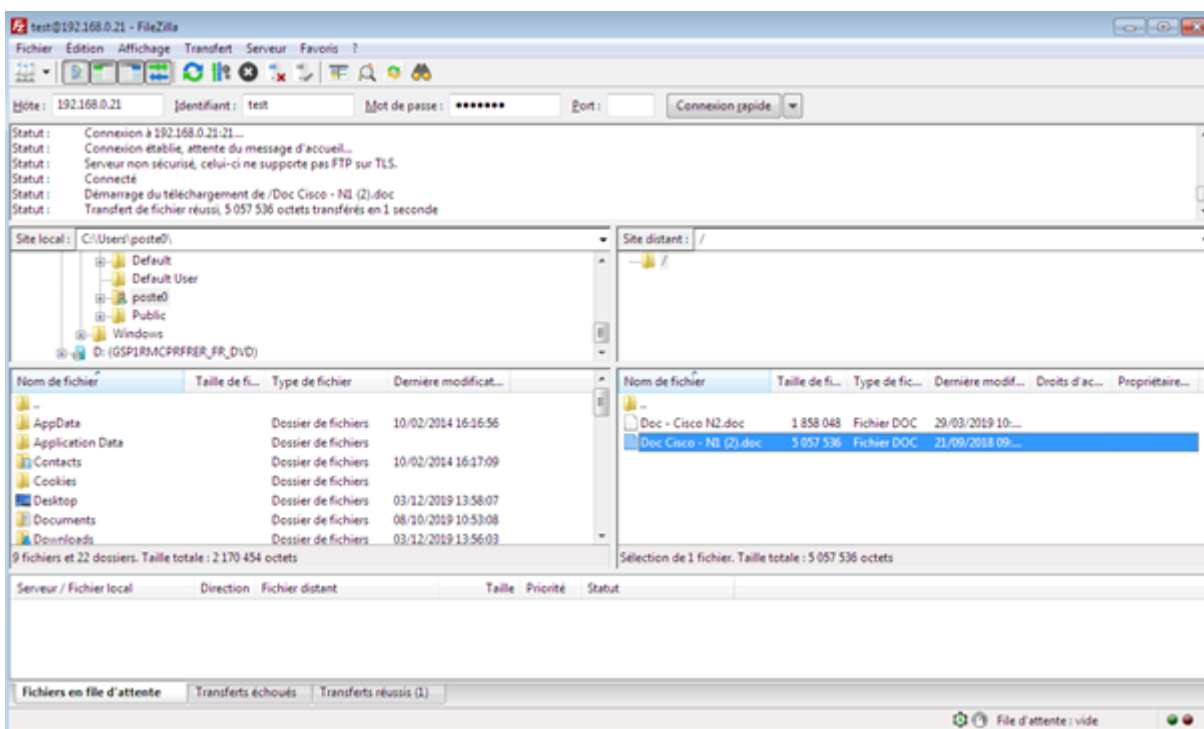


On choisit ensuite en cochant ou non les cases les permissions : lecture, écriture, suppression... Tout est prêt.



Sur la machine cliente, on entre dans « Hôte » l'adresse IP du serveur FTP, dans « Identifiant » le nom d'utilisateur, « Mot de passe » le mot de passe lié à l'utilisateur et le port (par défaut 21). On clique sur connexion rapide.

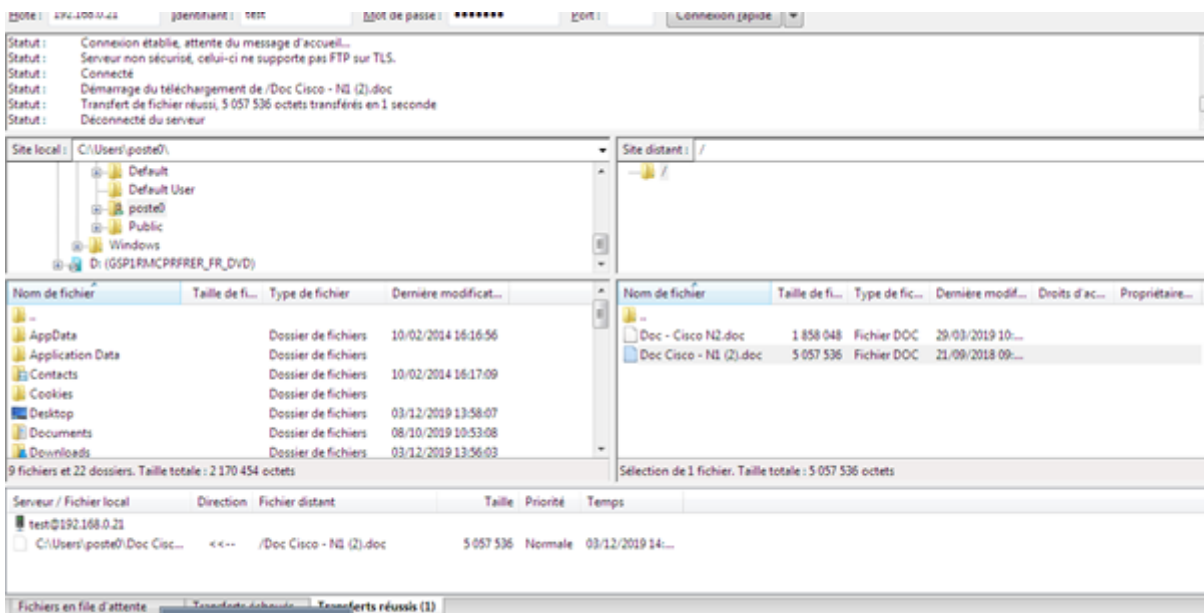
Un message s'affiche disant que la connexion n'est pas sécurisé. En effet, les logins ne sont pas protégés.



On a ensuite un dialogue nous confirmant la connexion.

Juste en dessous à gauche, on a site local : il s'agit de la destination de téléchargement des fichiers. A droite, le site distant correspondant au chemin des fichiers du serveur. Dans le serveur, dans cette exemple, nous avons deux fichiers.

On effectue un clic droit sur « Doc - Cisco N2.doc » par exemple, et télécharger. On a un message en bas à droite de l'écran nous confirmant la réussite du téléchargement.



Dans l'onglet « Transferts réussis » en bas de l'écran, on a une ligne par fichier, avec la destination de téléchargement, le fichier distant, la taille, la priorité et le temps.

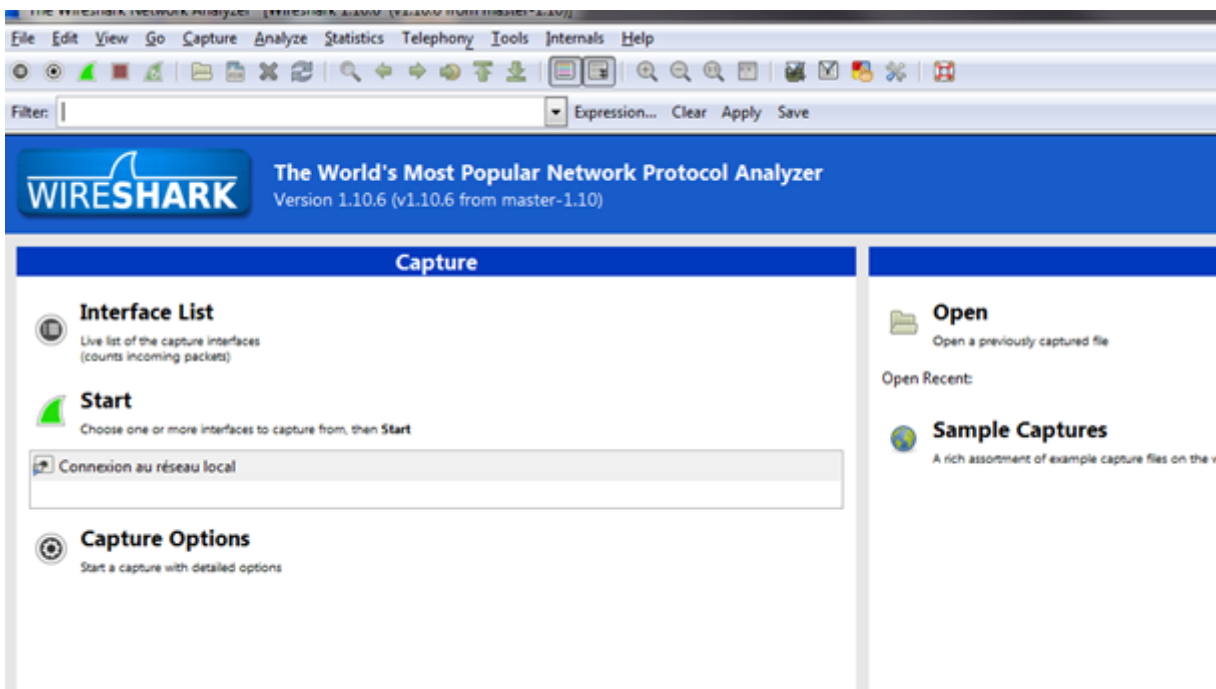
Du côté serveur, nous avons des lignes confirmant le téléchargement :

```
(000004)03/12/2019 14:19:10 -test (192.168.0.205)> RETR Doc Cisco - N1 (2).doc
(000004)03/12/2019 14:19:10 -test (192.168.0.205)> 150 Opening data channel for file download from server of "/Doc Cisco - N1 (2).doc"
(000004)03/12/2019 14:19:10 -test (192.168.0.205)> 226 Successfully transferred "/Doc Cisco - N1 (2).doc"
```

De même pour les connexions/déconnexions au serveur :

```
(000004)03/12/2019 14:19:10 - (not logged in) (192.168.0.205)> USER test
(000004)03/12/2019 14:19:10 - (not logged in) (192.168.0.205)> 331 Password required for test
(000004)03/12/2019 14:19:10 - (not logged in) (192.168.0.205)> PASS *****
(000004)03/12/2019 14:19:10 -test (192.168.0.205)> 230 Logged on
```

Afin de prouver la non sécurisation du FTP, nous pouvons utiliser Wireshark. Celui -ci va analyser et lister les trames du réseau.



Une fois le programme lancé, on va écrire « ftp » dans « Filter » afin de filtrer les trames. On aura donc les trames liées au protocole ftp d'affichées.

Une fois écrit, nous allons cliquer sur « Start ». On se connecte alors sur la machine physique au serveur. On peut ensuite arrêter la capture des trames.

On obtient le résultat suivant :

No.	Time	Source	Destination	Protocol	Length	Info
25705	11.59446900	192.168.0.21	192.168.0.205	FTP	197	Response: 220-Filezilla Server 0.9.60 beta
25706	11.59635400	192.168.0.205	192.168.0.21	FTP	64	Request: AUTH TLS
25707	11.59646000	192.168.0.21	192.168.0.205	FTP	99	Response: 502 Explicit TLS authentication not allowed
25708	11.59711100	192.168.0.205	192.168.0.21	FTP	64	Request: AUTH SSL
25709	11.59722700	192.168.0.21	192.168.0.205	FTP	99	Response: 502 Explicit TLS authentication not allowed
34049	14.41548500	192.168.0.205	192.168.0.21	FTP	65	Request: USER test
34050	14.41568400	192.168.0.21	192.168.0.205	FTP	86	Response: 331 Password required for test
34051	14.41687600	192.168.0.21	192.168.0.21	FTP	68	Request: PASS mdptest
34052	14.41714600	192.168.0.21	192.168.0.205	FTP	69	Response: 230 Logged on
34053	14.41756800	192.168.0.205	192.168.0.21	FTP	60	Request: SYST
34054	14.41769000	192.168.0.21	192.168.0.205	FTP	86	Response: 215 UNIX emulated by Filezilla
34055	14.41810100	192.168.0.205	192.168.0.21	FTP	60	Request: FEAT
34056	14.41827300	192.168.0.21	192.168.0.205	FTP	176	Response: 211-Features:
34057	14.42283500	192.168.0.205	192.168.0.21	FTP	60	Request: PWD
34058	14.42302600	192.168.0.21	192.168.0.205	FTP	85	Response: 257 "/" is current directory.
34059	14.42517000	192.168.0.205	192.168.0.21	FTP	62	Request: TYPE I
34060	14.42537100	192.168.0.21	192.168.0.205	FTP	73	Response: 200 Type set to I
34061	14.42594900	192.168.0.205	192.168.0.21	FTP	60	Request: PASV
34062	14.42642500	192.168.0.21	192.168.0.205	FTP	104	Response: 227 Entering Passive Mode (192,168,0,21,214,147)
34064	14.42794600	192.168.0.205	192.168.0.21	FTP	60	Request: MLSD
34069	14.42899500	192.168.0.21	192.168.0.205	FTP	109	Response: 150 opening data channel for directory listing of "/"
34072	14.42908500	192.168.0.21	192.168.0.205	FTP	88	Response: 226 Successfully transferred "/"

On peut y retrouver l'identifiant et le mot de passe de connexion. A la ligne 6, on a « USER test » ce qui correspond à « Identifiant : test ». L'identifiant de connexion est « test ».

Deux lignes en dessous, on a « PASS mdp test » ce qui correspond à « mot de passe : mdptest ».
Le mot de passe est donc « mdptest ».

Afin de sécuriser un serveur FTP, on doit utiliser un autre port que 21 et un certificat SSL en utilisant un protocole sécurisé.

Revision #2

Created 14 February 2021 11:32:53 by Khroners

Updated 30 March 2021 12:25:22 by Khroners