TP3 M2106

Table des matières

1) Connexion à un serveur FTP

1) Lorsque je tape ftp dans le terminal, je peux entrer depuis l'interface ftp :

```
test@214-3:~$ ftp
ftp>
```

2) Lorsque je tape help en étant dans la commande ftp je peux voir toutes les syntaxes qui sont reliées à cette commande

```
test@214-3:~$ ftp
ftp> help
Commands may be abbreviated.  Commands are:

!               dir             mdelete         qc              site
$               disconnect      mdir            sendport        size
account         exit            mget            put             status
append          form            mkdir           pwd             struct
ascii           get             mls             quit            system
bell            glob            mode            quote           sunique
binary          hash            modtime         recv            tenex
bye             help            mput            reget           tick
case            idle            newer           rstatus         trace
cd              image           nmap            rhelp           type
cdup            ipany           nlist           rename          user
chmod           ipv4            ntrans          reset           umask
close           ipv6            open            restart         verbose
cr              lcd             prompt          rmdir           ?
delete          ls              passive         runique
debug           macdef          proxy           send
```

TP3 M2106

Les syntaxes principales sont : delete, disconnect, exit, open, reset, quit, help et restart.

3) Pour se connecter au serveur ftp je dois me mettre dans l'interface ftp et j'utilise la commande suivante :

```
ftp> open 10.214.1.1
Connected to 10.214.1.1.
220 (vsFTPd 3.0.3)
Name (10.214.1.1:test): test
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

4) Tous les utilisateurs en interface ftp peuvent y accéder mais il faut savoir le nom de l'utilisateur et le mot de passe de la machine. Les anonymes ne peuvent pas se connecter.

En cas de succès le message retourné est le suivant :

```
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

En cas d'échec le message retourné est le suivant :

```
530 Login incorrect.
Login failed.
```

5) Pour savoir où je me trouve sur la machine distante j'effectue la commande suivante :

```
ftp> pwd
257 "/" is the current directory
```

Pour savoir où je me trouve avec la machine locale j'effectue la commande suivante :

```
ftp> !pwd
/home/test
```

6) Oui je peux créer un répertoire sur le serveur grâce à la commande suivante :

```
ftp> mkdir tp3
```

TP3 M2106

```
257 "/tp3" created
```

7) Pour envoyer un fichier sur le serveur, je peux utiliser 2 commandes :

```
ftp> send test
local: test remote: test
200 PORT command successful. Consider using PASV.
553 Could not create file.
```

```
ftp> put test2
local: test2 remote: test2
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
```

8) Je peux prendre un fichier du serveur avec la commande suivante :

```
ftp> get test
local: test remote: test
200 PORT command successful. Consider using PASV.
550 Failed to open file.
```

9) Quand je me déconnecte du serveur il me retourne le message suivant :

```
ftp> close
221 Goodbye.
```

2) Capture de trames en mode actif

1) Je lance wireshark. Je lance la capture de trame. En arrivant dans la capture je met le filtre d'affichage suivant : ip.addr == 10.214.3.1 and ip.addr == 10.214.1.1

Je retourne dans le terminal et je relance une connexion au serveur :

```
ftp> open 10.214.1.1
Connected to 10.214.1.1.
220 (vsFTPd 3.0.3)
Name (10.214.1.1:test): test
```

TP3 M2106

```
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

Les ports mis en jeu sont le 21 (FTP) et le 35878 (Utilisateur).

L'utilisateur est celui qui initie le dialogue car c'est lui qui demande à se connecter au serveur.

Je suit le flux et j'obtiens :

220 (vsFTPd 3.0.3)
USER test
331 Please specify the password.
PASS test
230 Login successful.
SYST
215 UNIX Type: L8

Au vu des trames on peut dire que la connexion est peu sécurisée car en mode actif le port du serveur reste le même.

2) Lorsque j'effectue un ls sur le serveur, le flux TCP est le suivant :

PORT 10,214,3,1,177,207

200 PORT command successful. Consider using PASV.

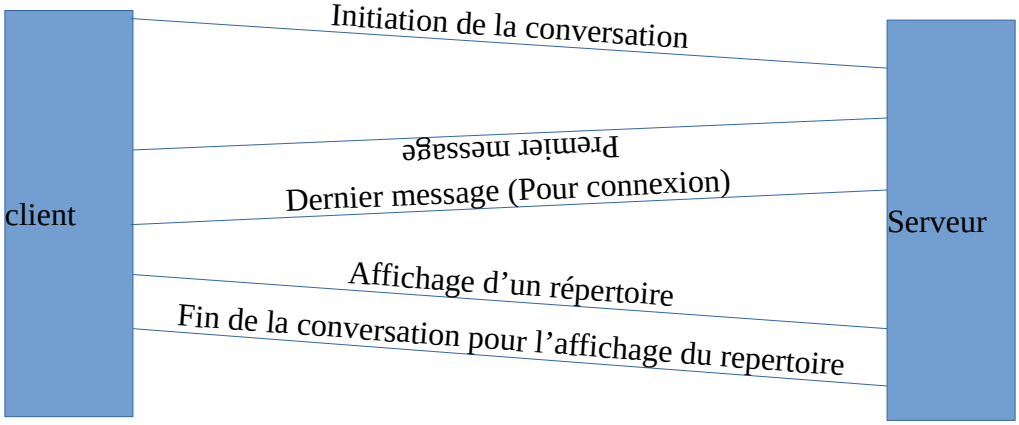
LIST

150 Here comes the directory listing.

226 Directory send OK.

Les ports mis en jeu sont encore les mêmes. L'utilisateur initie encore la communication.

3)



TP3 M2106

3) Captures de trames en mode passif

1. Pour passer en mode passif, dans l'interface ftp on entre la commande « passive ».

```
ftp> passive
Passive mode on.
```

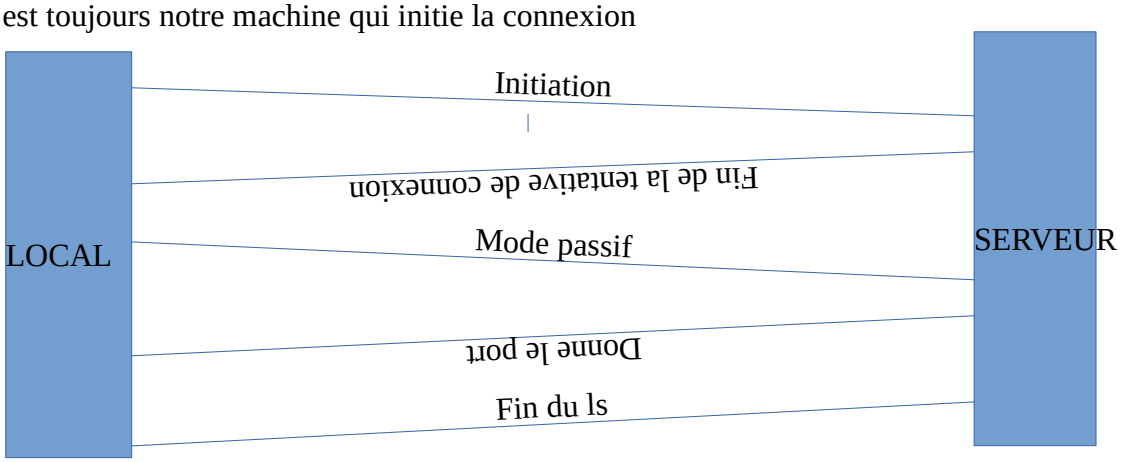
2. Avec le mode passif, je refais la même manipulation. Ci-dessous, on voit le flux TCP et on voit que la seule différence est que notre Machine (lorsqu'on fait le ls) dit qu'elle est en mode passif.

Elle dit « PASV » et cette fois, c'est le serveur qui répond et qui donne un port.

```
20 (vsFTPd 3.0.3)
USER test
331 Please specify the password.
PASS test
230 Login successful.
SYST
215 UNIX Type: L8
PASV
227 Entering Passive Mode (10,214,1,1,63,88).
LIST
150 Here comes the directory listing.
226 Directory send OK
```

Le graphique des flux est le même sauf pour la requête de port, qui est faite par le serveur maintenant.

C'est toujours notre machine qui initie la connexion



TP3 M2106

3. Les deux modes de fonctionnement sont similaires. La seule chose qui change est lorsque le client effectue une action en mode actif, il donne le port au serveur alors qu'en mode passif c'est le serveur qui donne le port.