Comunicacions segures

UF2 - Instal·lació i administració de serveis de transferència de fitxers

Comunicacions segures

Quan es va dissenyar FTP no es va tenir en compte la seguretat més enllà de l'usuari i la contrasenya. Per això diem que:

FTP no és segur!!!

La informació viatja en text pla, sense encriptar. Qualsevol pot capturar els paquets i espiar les dades.

Comunicacions segures

S'han afegit extensions per tal de xifrar les comunicacions:

- FTPS (FTP sobre SSL)
- SFTP (extensió de SSH)

FTPS

FTPS (FTP sobre SSL/TLS) utilitza la capa de seguretat SSL per fer que les comunicacions siguin xifrades. Igual que HTTPS!

Proporciona la confidencialitat i autenticació necessàries per les comunicacions FTP.

En aquest cas, utilitzem els mateixos ports que per FTP (20 i 21).

FTPS

vsftpd porta preparats uns certificats per poder xifrar les comunicacions, però els podem substituir per altres.

Per activar el protocol FTPS cal descomentar les línies següents:

```
ssl_enable=yes
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
```

FTPS

```
ssl_enable=yes
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
```

- **ssl_enable:** habilita SSL per activar FTPS.
- **rsa_cert_file:** conté el certificat públic.
- **rsa_private_key_file:** conté la clau privada.

FTPS

El client ftp no suporta SSL, per això caldrà instal·lar un altre client de text:

- ftp-ssl o lftp.

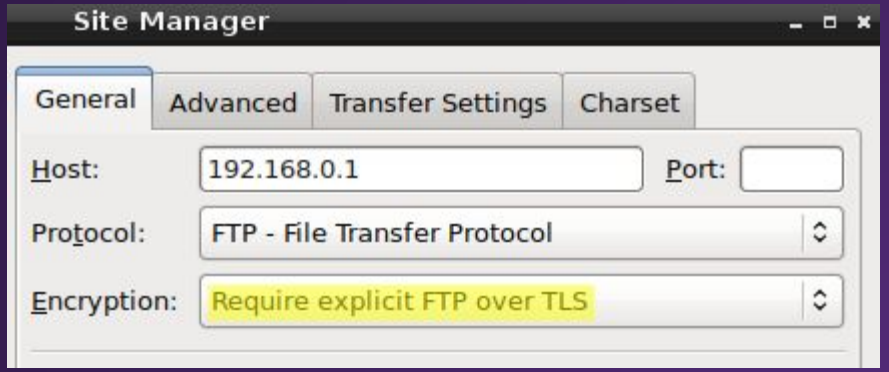
```
usuari@client:~$ ftp 10.0.2.15
Connected to 10.0.2.15.
220 (vsFTPd 3.0.3)
Name (10.0.2.15:usuari): usuari
530 Non-anonymous sessions must use encryption.
Login failed.
421 Service not available, remote server has closed connection
ftp> quit
```

FTPS

Des de ftp-ssl podem accedir al servidor.

També des de clients gràfics! (ex. Filezilla)

```
usuari@client:~$ ftp-ssl 10.0.2.15
Connected to 10.0.2.15.
220 (vsFTPd 3.0.3)
Name (10.0.2.9:usuari): usuari
234 Proceed with negotiation.
[SSL Cipher ECDHE-RSA-AES256-GCM-SHA384]
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```



SFTP

És una implementació diferent del protocol FTP.

És una extensió del protocol SSH, que és el que ofereix el xifrat.

El protocol SFTP utilitza el port 22 (el de SSH).

NO ÉS COMPATIBLE AMB FTPS!

SFTP

No confondre amb SFTP (Simple Mail Transfer Protocol)!

Per poder utilitzar SFTP cal instal·lar un altre programari, per exemple openSSH, que incorpora un servidor FTP.

Però per aquest ja ens podrem connectar amb qualsevol client FTP.

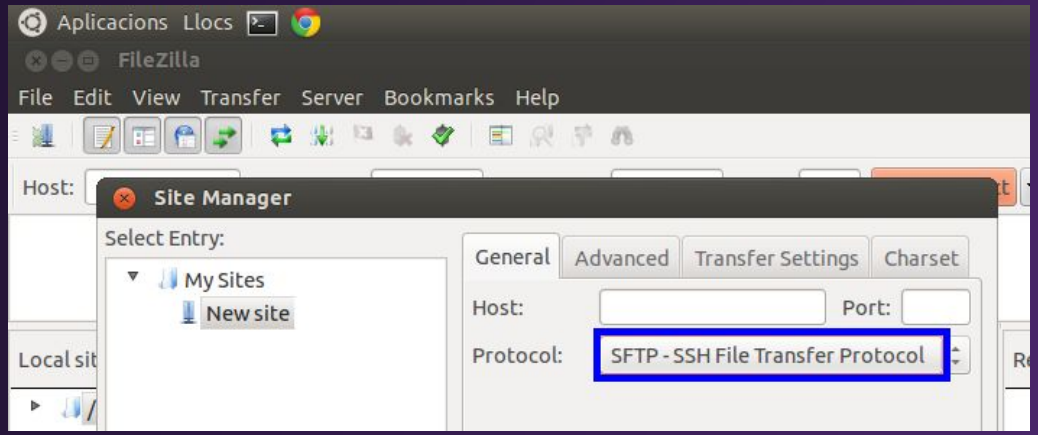
SFTP

Ens connectarem a SFTP amb la comanda SFTP i la ip.

```
usuari@client:~$ sftp 10.0.2.15
The authenticity of host '10.0.2.15 (10.0.2.15)' can't be established.
ECDSA key fingerprint is SHA256:2cqYKzks+fFtaQutgx8jLfvy8X08lEzxgPdkXYg2DKw.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.2.15' (ECDSA) to the list of known hosts.
usuari@10.0.2.15's password:
Connected to 10.0.2.15.
sftp>
```

SFTP

En cas de voler-nos connectar des d'un client gràfic cal especificar que utilitzarem SFTP. (Ex. Filezilla):



TFTP

Servei de transferència trivial de fitxers

TFTP

El protocol TFTP (trivial file transport protocol) proporciona un servei de transferència de fitxers més bàsic i elemental que FTP.

És simple!

No permet autenticació ni incorpora mecanismes de seguretat.

Només permet baixar i pujar fitxers.

TFTP

TFTP va ser ideat per baixar fitxers en entorns simples com la iniciació d'estacions de treball sense sistema operatiu.

S'utilitza en entorns que no hi ha el programari necessari per utilitzar FTP.

TFTP

Les utilitats de TFTP són:

- inicialitzar estacions de treball sense disc, permetent carregar el SO per TFTP.
- Desar i baixar configuracions. Ex: fitxers de configuració de xarxa, d'encaminadors...
- Iniciar instal· lacions de SO per xarxa. Els equips es baixen per TFTP el programari d'instal· lació.

TFTP

Els repositoris TFTP són públics!

Es troben al directori /tftpboot. Qualsevol client pot accedir al seu contingut.

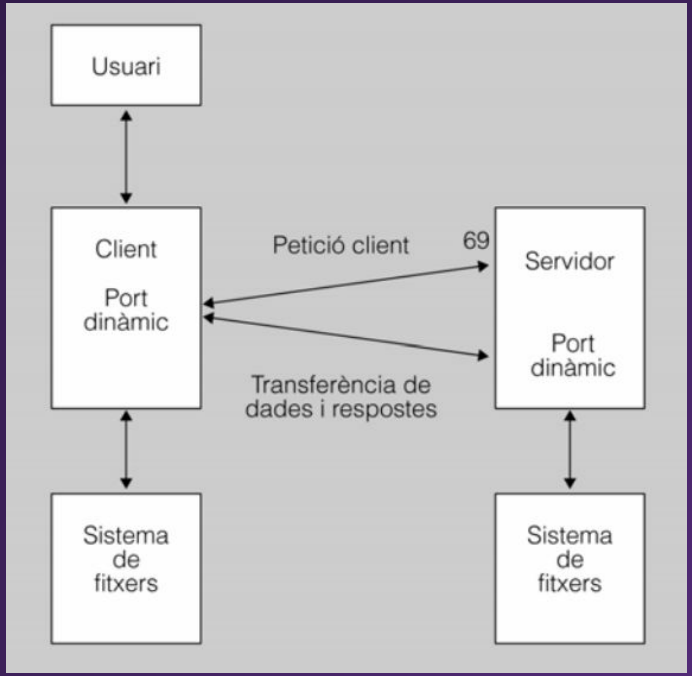
Les accions del client dependràn dels permisos que tingui.

TFTP

TFTP és un protocol de capa d'aplicació.

Utilitza UDP en la capa de transport!

UDP es diferencia amb TCP perquè s'envien datagrames de 512 bytes de màxim.



TFTP

No existeix un flux de dades constant entre client i servidor.

Els protocols basats en UDP no realitzen un lliurament garantit dels datagrames que transporten.

La fiabilitat s'implementa mitjançant temporitzadors d'espera.

TFTP

TFTP utilitza el port 69 per escoltar les peticions entrants dels clients.

Si el servidor pot respondre, ho farà indicant un nou port, per on es realitzarà la tranferència de dades.

TFTP

TFTP té els següents tipus de paquets:

- **RRQ:** read request. El client l'envia per sol·licitar al servidor el fitxer a baixar.
- **WRQ:** write request. El client l'envia al servidor per indicar el nom del fitxer a pujar.
- **DATA:** dades. Blocs de dades de 512 bytes amb el contingut del fitxer.
- **ACK:** acknowledgment. S'envia per confimar la recepció d'un paquet.
- **Error:** error. Indica que s'ha produït un error.

TFTP

```
$tftp localhost
tftp> verbose
tftp> trace
tftp> status
      Connected to 127.0.0.1.
      Mode: netascii Verbose: on Tracing: on
      Rexmt-interval: 5 seconds, Max-timeout: 25 seconds
tftp> get hola.txt
      getting from 127.0.0.1:hola.txt to hola.txt [netascii]
      sent RRQ <file=hola.txt, mode=netascii>
      received DATA <block=1, 85 bytes>
      Received 85 bytes in 0.9 seconds [774 bit/s]
tftp> put nou.doc carta.txt
      putting nou.doc to 127.0.0.1:carta.txt [netascii]
      sent WRQ <file=carta.txt, mode=netascii>
      received ACK <block=0>
      sent DATA <block=1, 72 bytes>
      received ACK <block=1>
      Sent 72 bytes in 0.5 seconds [1140 bit/s]
tftp> quit
```