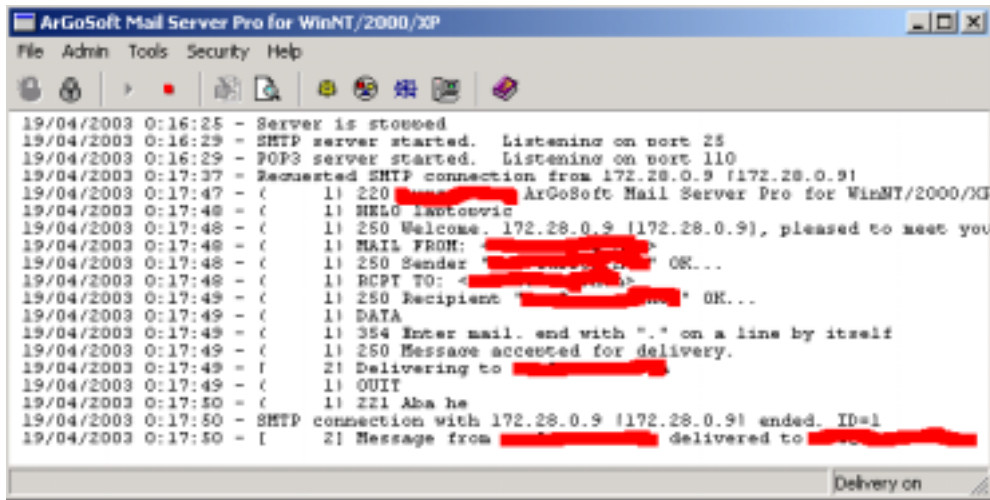


**\*\*\* RECUERDA NO EJECUTAR EL COMANDO STOR, QUE SINO NO TE FUNCIONARÁ!!!!**

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 lacoovic
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 - I 2) Delivering to [redacted]
19/04/2003 0:17:49 - C 1) QUIT
19/04/2003 0:17:50 - C 1) 221 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>

## Práctica 30. Túneles y Redirectores de puertos (Por HxC Mods-Adm)

Bueno, los **redirectores de puertos en realidad son bouncers**.

Vamos a ver tres, con sus pequeñas diferencias y su parte de explicación

*Rinetd, fpipe y pptunnel, en*

*Rinetd* redirige las conexiones TCP desde una dirección y puerto local hacia otra dirección y puerto remoto.

Debemos crear un archivo de configuración con las direcciones IP y puertos TCP necesarios, por ejemplo:

**Dirección Local: 1.2.3.4**  
**Puerto Local: 1234**  
**Dirección Remota: 55.55.55.55**  
**Puerto Remoto: 5555**

El archivo de configuración sería:

*1.2.3.4 1234 55.55.55.55 5555*

Se trata de un archivo de texto que se pasa como parámetro a *rinetd -c archivo.txt*

### Ejemplo práctico.

Supongamos que tenemos la máquina 172.28.5.25 comprometida (bajo nuestro control) y deseamos “atacar” otra máquina cuya IP es 172.28.99.99, la cual es un servidor web al que queremos “introducimos” mediante un bug como alguno descubierto para *Unicode*.

Nuestro ordenador (desde el cual realizamos “el asalto”) tiene como dirección IP 172.28.0.1, si accedemos directamente al Servidor web, en su registro de sucesos (logs web) quedaría registrada nuestra propia dirección IP aunque sólo sea por el hecho de visitar su página sin ninguna otra intención, sin embargo si conseguimos ejecutar rinetd en el ordenador “comprometido” (172.28.5.25) será ésta la única dirección registrada y no la nuestra.

El archivo de configuración podría ser:

Archivo.txt *172.28.5.25 80 172.28.99.99 80*

La instrucción a ejecutar en la máquina 172.28.5.25 sería:

*Rinetd -c archivo.txt*

Después desde nuestro Internet Explorer escribiríamos en la barra de dirección: <http://172.28.5.25>

**FIJATE BIEN:** la máquina 172.28.5.25 escucha por el puerto 80 la conexiones entrantes y las redirecciona por el mismo puerto 80 al servidor web (172.28.99.99) que registrará ese acceso.

*¿Y si cambiamos los puertos, por ejemplo por el 25? Pues que si la máquina remota es un servidor SMTP podremos enviar CORREO BAJO BANDERA DE LA MAQUINA BOUNCEADA.*

Bueno el resto de ideas y usos los dejo a tu propio estudio.