Universidad de Alcalá

Departamento de Automática

ARQUITECTURA DE REDES
Laboratorio

Práctica 5: Ejercicios de aplicación de FTP.

Grado en Ingeniería Informática
Curso 2022/23

1. OBJETIVOS.

El objetivo de esta práctica es que el alumno llegue a conocer los principales conceptos relacionados con la comunicación de procesos utilizando protocolos *FTP*.

2. ACTIVIDADES.

- Presentación y estudio de una aplicación útil para el acceso a los servidores FTP en ausencia de un programa cliente, denominada ***Netcat***.
- Estudio del protocolo de aplicación FTP.
- El alumno deberá estudiar con la aplicación Wireshark los resultados de las capturas de tráfico de red obtenidas a partir de las transferencias de datos realizadas.

3. EJERCICIOS.

3.1 Introducción: Modos de operación del protocolo FTP.

A diferencia del protocolo HTTP, en el que se emplea una sola conexión para transmitir información de control y datos (señalización en banda), el protocolo FTP se sirve de dos conexiones independientes, una para control y otra para datos (señalización fuera de banda).

Atendiendo a las características del protocolo FTP, la conexión de control se cursa, típicamente, a través del puerto 21 del servidor; la conexión de datos a través del puerto 20 del servidor. No obstante, el establecimiento de la conexión de datos exhibe ciertas particularidades, dependiendo del modo de funcionamiento del protocolo FTP: modo activo y modo pasivo.

3.1.1 Modo activo

En el modo activo el cliente FTP se conecta al puerto de control del servidor (puerto 21) mediante un puerto no privilegiado[1]. Este puerto no privilegiado es asignado automáticamente por el propio Sistema Operativo, con **N > 1024**, simbolizando **N** el puerto escogido. Por tanto, el par de puertos (**N**, 21) caracteriza la conexión de control, establecida entre el cliente y el servidor.

Respecto a la conexión de datos, el cliente suele seleccionar el puerto **N+1**, y el servidor, por defecto, el puerto 20. Así, la conexión de datos queda caracterizada por el par de puertos (**N**+1, 20), si bien cabe destacar que es el servidor el que inicia la conexión de datos (ver Figura 1).

Figura 1: Modo activo.

(1) La arquitectura TCP/IP identifica los puertos privilegiados como aquellos puertos reservados, de mutuo acuerdo, a los protocolos estándar (puertos en el rango 0-1023). Actualmente, en la siguiente dirección Web http://www.iana.org/ puede consultarse un listado de los puertos privilegiados comúnmente aceptados

Si el cliente decide utilizar un puerto diferente a **N**+1, debe notificárselo al servidor mediante los comandos **PORT** o **EPRT,** cursados a través de la conexión de control, indicando el nuevo puerto de transferencia de datos **M**. De esta forma, la nueva configuración de la conexión de datos queda caracterizada por el par de puertos (**M**, 20).

La sintaxis del comando **PORT** obedece a **`PORT a1,a2,a3,a4,p1,p2`**, donde `a1,a2,a3,a4` identifica los cuatro octetos (formato decimal) de la dirección IP a la que debe conectarse el servidor para cursar la transferencia de datos, y `p1,p2` los valores que permiten determinar el puerto, (`puerto=p1•256+ p2`).

La sintaxis del comando **EPRT** obedece a **`EPRT |1| a1,a2,a3,a4|puerto|`**, donde el dígito **`1`** indica que se opera con IPv4, `a1,a2,a3,a4` identifica los cuatro octetos (formato decimal) de la dirección IP a la que debe conectarse el servidor para cursar la transferencia de datos y `puerto` el puerto de datos del cliente.

3.1.2 Modo pasivo.

En el modo activo el servidor inicia la conexión de datos. Si la infraestructura del cliente está protegida por un firewall, es más que probable que éste bloquee la conexión del servidor, puesto que puede comprometer la seguridad de la red interna. En otros términos, el firewall normalmente impide las conexiones procedentes de la red externa, pero autoriza las conexiones desde la red interna hacia la red externa.

El modo pasivo elude este inconveniente estableciendo que *sea el cliente el que inicie la conexión de datos*, esto es, el cliente es el responsable de iniciar la conexión de control y la conexión de datos. En este sentido el cliente está obligado a comunicar explícitamente al servidor su voluntad de configurar la transferencia de datos en modo pasivo.

Una vez establecida la conexión de control entre el cliente y el servidor, a través del par de puertos (**N**, 21), y antes de proceder con cualquier transferencia de datos, el cliente debe enviar al servidor el comando **EPSV** o el comando **PASV**. Con estos comandos el servidor concluye que la transferencia de datos torna a modo pasivo, por lo que ha de seleccionar un puerto **S > 1024** y notificárselo al cliente a través de la conexión de control. De esta forma, la configuración de la conexión de datos queda caracterizada inequívocamente por el par de puertos (**N**+l, **S**), como ilustra la Figura 2.

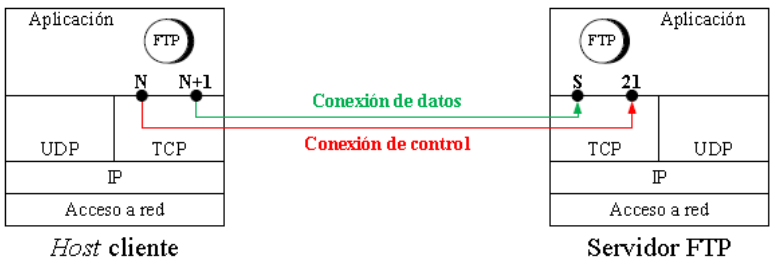

Figura 2: Modo pasivo.

3.2. Análisis de una sesión FTP mediante Wireshark

Se va a realizar el estudio de una sesión FTP establecida entre un cliente FTP estándar, disponible en la mayoría de las distribuciones de Linux, y un servidor FTP, gestionado por el *Departamento de Ciencias de la Computación*, en base a las capturas efectuadas por el analizador de red Wireshark.

Se suministra a modo de ejemplo, la captura de una sesión FTP practicada desde un Terminal de Linux (*capturaftp.libcap*). El archivo *sesionftp.pdf* reúne la sesión FTP en la que se fundamenta la captura distribuida. En este archivo las órdenes introducidas por teclado figuran en negrita.

EJERCICIO 1: ***Procedimiento de captura mediante Wireshark.***

Se procede a detallar el procedimiento que le permitirá examinar los mensajes FTP y los segmentos TCP intercambiados entre un *host* cliente y un servidor FTP.

1) Inicie un Terminal de Linux. Cerciórese que el navegador Web no esté operativo ni ninguna otra aplicación de red que pueda entorpecer la captura de interés.

2) Ejecute el software Wireshark e inicie la captura de tráfico.

3) Introduzca el siguiente comando en la línea de órdenes de su Terminal de Linux.

```
ftp nic.funet.fi | tee sesionftp
```

*(**nic.funet.fi** es un repositorio de software de Linux. Se puede comprobar en https://www.nic.funet.fi/).*

El servidor FTP solicita un nombre de usuario **Anonymous,** y opcionalmente puede solicitar una palabra de paso (password) **anonymous.**

El comando introducido *(tee sesionftp)* guarda toda la información en el archivo `sesionftp`.

La lista de comandos FTP, está en: *http://www.nsftools.com/tips/RawFTP.htm*

4) Finalice la captura y asegúrese que el software Wireshark sólo muestre segmentos TCP y mensajes FTP (cadena de filtrado: **tcp**).

5) Analice los campos contenidos en los mensajes FTP, y los segmentos TCP capturados de las órdenes introducidas por teclado en el proceso de comunicación con el servidor FTP, y las trazas de Wireshark de las que se ha extraído la información (ver sesionftp.pdf)

3.3 Ejecución del protocolo FTP mediante Netcat.

En este apartado se estudia la forma de dialogar directamente con un servidor FTP, sin necesidad de recurrir a un programa cliente, específicamente diseñado para tal cometido, mediante la herramienta GNU de libre distribución *Netcat*.

La herramienta *Netcat* permite leer y escribir datos sobre una conexión de red que opere bajo la arquitectura TCP/IP. Ofrece un amplio abanico de posibilidades, si bien esta actividad se limita a aquellas facilidades destinadas al establecimiento de conexiones TCP.

La herramienta *Netcat* admite configurar el sistema para que actúe como cliente o como servidor. Si se desea que ejerza como cliente, para conectarse a un servidor de nombre *server*, que escucha en el puerto *port number*, se emplea la sintaxis

```
nc server port_number
```

Si, por el contrario, se pretende que ejerza como servidor, escuchando (atributo -l, donde l significa *listen*) en el puerto *port number*, se utiliza la sintaxis

```
nc -1 -p port_number
```

EJERCICIO 2: ***Conexión de control en FTP***

Para conectarse a un servidor FTP y, de esta forma, habilitar la posibilidad de enviar comandos a través de la conexión de control, según el listado publicado en http://www.nsftools.com/tips/RawFTP.htm. Se procederá de la siguiente manera:

1) Inicie un Terminal de Linux e introduzca el siguiente comando en la línea de órdenes:

   ```
   nc nic.funet.fi 21
   ```

   Con esta orden queda establecida la conexión de control, por lo que se está en disposición de enviar comandos que pueda interpretar el servidor FTP.

   *La sintaxis de Netcat para acceder a la ayuda donde nos mostrará todos sus comandos, utiliza el parámetro "-h" (**nc –h**).*

2) El servidor FTP se mantiene a la espera de que el usuario se autentique con un nombre de usuario (comando USER) y una password (comando PASS). En el caso del servidor FTP *nic.funet.fi*

   ```
   USER anonymous
   PASS anonymous
   ```

   Una vez autenticados, ya se puede dialogar con el servidor FTP.

   - Con objeto de determinar el directorio de trabajo actual en el servidor, se emplea el comando **PWD**.

   - Con objeto de listar el contenido del directorio de trabajo actual en el servidor, se emplea el comando **STAT/**. Una vez identificados los subdirectorios disponibles, es posible cambiarse a alguno de ellos mediante el comando

     ```
     CWD nombre_subdirectorio.
     ```

3) Ejecute el software Wireshark e inicie la captura de tráfico en las siguientes operaciones.

4) Intenta averiguar de qué conexión (control o datos) se sirve el servidor FTP para exportar las respuestas a los comandos **PWD, STAT /** y **CWD**.

5) El comando que permite listar el contenido de un directorio es **LIST**, en lugar de **STAT /.** Pruebe el comando **LIST** y analice la respuesta que remite el servidor FTP.

6) Finalice la captura y asegúrese que el software Wireshark sólo muestre segmentos TCP y mensajes FTP (cadena de filtrado: **tcp**).

7) Analice los campos contenidos en los mensajes FTP, y los segmentos TCP capturados de las órdenes introducidas por teclado en el proceso de comunicación con el servidor FTP.

EJERCICIO 3: *Conexión de datos en FTP.*

La transferencia de datos entre el cliente y el servidor FTP debe configurarse en modo pasivo o en modo activo.

1. Modo pasivo

En el modo pasivo el cliente debe iniciar la conexión de datos sobre el *puerto **S*** que el servidor le notifique a través de la conexión de control (ver apartado 3.1.2).
Por tanto, se procederá de la siguiente manera:

1) El cliente debe averiguar el puerto de datos, conforme a uno de los siguientes comandos:

   - ***Opción 1:***

     Introduzca el comando **PASV**. La respuesta del servidor a este comando se asemeja a:

     ```
     227 Entering Passive Mode (193,166,3,1,154,61).(*)
     ```

     La información exhibida indica que el servidor FTP, con dirección IP 193.166.3.1, escucha en el puerto TCP 39485, esto es, 154·256+61.

   - ***Opción 2:***

     Introduzca el comando **EPSV**. La respuesta del servidor a este comando se asemeja a:

     ```
     229 Entering Extended Passive Mode (|||39485 |).
     ```

     La respuesta retorna directamente el número de puerto (39485). El resto de parámetros se omite, de lo que se deduce que la dirección IP coincide con la dirección IP sobre la que se ha establecido la conexión de control.

(*) Las direcciones IP son orientativas ya que pueden variar sin previo aviso, y ser diferentes para la Intranet y para Internet. Para saber cuales utilizar puedo emplear los comandos *ping nic.funet.fi*, o bien *nslookup nic.funet.fi*

2) Una vez conocido el puerto de datos del servidor FTP, **inicie otro Terminal de Linux**, con objeto de establecer la conexión de datos, e introduzca en la línea de órdenes

```
nc nic.funet.fi 39485
```

En este Terminal de Linux se mostrará la información transferida por la conexión de datos, de acuerdo con los comandos de control que el cliente ejecute en el Terminal de Linux sobre el que se ha establecido la conexión de control.

3) Introduzca el comando **LIST** en el terminal de Linux en el que se ha iniciado la conexión de control y verifique que sucede.

4) Con el comando **CWD** cámbiese al directorio *pub/FreeBSD* y, mediante el comando **RETR** *nombre_archivo* *(en minúsculas)*, descárguese un archivo a través de la conexión de datos. Observe los resultados obtenidos. En nuestro caso descargamos el fichero que se encuentra en este subdirectorio, denominado README.TXT

2. Modo activo

En el modo activo el servidor FTP debe iniciar la conexión de datos sobre el *puerto **M*** que el cliente le notifique a través de la conexión de control (ver apartado 3.1.1). Para ello, se procederá de la siguiente manera:

1) El cliente debe transferir el puerto de datos al servidor FTP, conforme a uno de los siguientes comandos:

   - ***Opción 1:***

     Después de establecer la conexión (Utilice como servidor FTP la dirección 128.10.252.10), introduzca el comando:

     ```
     PORT a1,a2,a3,a4,p1,p2
     ```

     Identificando *a1,a2,a3,a4* la dirección IP del cliente, y *p1•256+p2* el número de puerto que propone el cliente para la conexión de datos.

     Por ejemplo:

     ```
     PORT 128,10,252,10,20,50 (*)
     ```

   - ***Opción 2:***

     Después de establecer la conexión (utilice la dirección 128.10.252.10), introduzca el comando:

     ```
     EPRT |1|a1.a2.a3.a4 |puerto|
     ```

     Identificando el dígito *1* que se opera con **IPv4,*a1.a2.a3.a4*** la dirección IP del cliente, y *puerto* el número de puerto que propone el cliente para la conexión de datos.
     Por ejemplo:

     ```
     EPRT |1|128.10.252.10|5170|
     ```

2) Una vez notificado el puerto de datos al servidor FTP, inicie otro Terminal de Linux, con objeto de establecer la conexión de datos, e introduzca en la línea de órdenes:

```
nc -l 5170
```

En este Terminal de Linux se mostrará la información transferida por la conexión de datos, de acuerdo con los comandos de control que el cliente ejecute en el Terminal de Linux sobre el que se ha establecido la conexión de control.

3) Introduzca el comando **LIST** en el Terminal de Linux en el que se ha iniciado la conexión de control. Observe las diferencias que pueden establecerse respecto al modo pasivo.

5) Con el comando **CWD** cámbiese al directorio *pub/dict* y, mediante el comando **RETR** *nombre_archivo*, descárguese un archivo a través de la conexión de datos. Observe las diferencias que pueden establecerse respecto al modo pasivo. En nuestro caso descargamos el fichero que se encuentra en este subdirectorio, denominado README.txt

4. Bibliografía.

Gran parte del material de esta práctica ha sido proporcionado por Javier de Pedro Carracedo.

NOTA:

A continuación, se exponen algunas direcciones de servidores FTP en Internet, que se pueden utilizar también para realizar la práctica.

- 128.10.252.10 (puerto 21)
  ftp://128.10.252.10/

  a) ftp://128.10.252.10/pub/doc/dir-tree.doc

  b) ftp://128.10.252.10/pub/lists/README.txt

- 130.206.13.2 (puerto 21)
  ftp://130.206.13.2/

  a) ftp://130.206.13.2/debian/README.txt

  b) ftp://130.206.13.2/debian/README.mirrors.txt