UNIVERSIDAD ICESI
FACULTAD DE INGENIERÍA
REDES DE COMPUTADORES II
LABORATORIO – EL PROTOCOLO FTP

MOTIVACIÓN

FTP fue uno de los primeros protocolos de aplicación que se implementaron sobre la Internet, para permitir la transferencia de archivos. Aún es ampliamente utilizado en:

- Gestión de sitios web alojados en servicios de hosting
- Repositorios de software
- Envío de archivos, cuando el correo electrónico o la web resultan inconvenientes para este propósito

OBJETIVOS

Al finalizar la presente práctica, el estudiante estará en capacidad de:

- Describir la arquitectura (o modelo) empleado por el protocolo FTP.
- Emplear los comandos básicos de FTP para efectuar operaciones tales como entrada al sistema, cambio de directorio, listar el contenido de un directorio, recuperar un archivo o transferir un archivo.
- Entender la estructura y el significado de los códigos de estado que devuelve un servidor FTP.
- Diferenciar las dos modalidades principales de funcionamiento de FTP (activa y pasiva), y determinar cuál modalidad es la adecuada para una cierta aplicación.
- Comprender cómo están implementados un servidor y un cliente FTP.

INSUMOS NECESARIOS

Para completar la práctica se requiere lo siguiente:

- Una versión actualizada de Wireshark.
- Una versión actualizada de Filezilla (cliente FTP, disponible en https://filezilla-project.org/)
- Un navegador de Internet

PREPARACIÓN

Como preparación para la práctica, deben estudiarse los siguientes documentos:

- RFC 959 – File Transfer Protocol (https://tools.ietf.org/html/rfc959)
- RFC 2228 – FTP Security Extensions (https://tools.ietf.org/html/rfc2228)
- RFC 3659 – Extensions to FTP (https://tools.ietf.org/html/rfc3659)

Tras el estudio de los documentos, deben contestarse las siguientes preguntas:

1. ¿Cuál es la arquitectura (o modelo) que emplea el protocolo FTP para implementar el servicio de transferencia de archivos?
2. ¿Cuáles son los comandos de control de acceso de FTP? Explique brevemente cada uno de ellos.
3. ¿Cuáles son los comandos que fijan parámetros de transferencia de datos en FTP? Explique brevemente cada uno de ellos.
4. ¿Cuáles son los comandos de servicio de FTP? Explique brevemente cada uno de ellos.
5. Explique la estructura de los códigos de respuesta de FTP.
6. Como mínimo, ¿qué comandos debe procesar un servidor de FTP?
7. ¿Qué comandos incluye la RFC 2228? Explíquelos brevemente.
8. ¿Qué comandos nuevos incluye la RFC 3659? Explíquelos brevemente.

ANÁLISIS DE UNA SESIÓN DE FTP EN MODALIDAD PASIVA

Cargue en Wireshark el archivo `FTP_Pasivo.pcapng`, que podrá encontrar en Moodle. Este archivo contiene una sesión completa del protocolo FTP, en 8 flujos TCP:

ID Flujo	Contenido
0	Solicitud del directorio raíz
1	Contenido del directorio raíz
2	Solicitud del directorio `/Datecsa`
3	Contenido del directorio `/Datecsa`
4	Solicitud del directorio `/Datecsa/Driver 64 bits`
5	Contenido del directorio `/Datecsa/Driver 64 bits`
6	Solicitud del archivo `KMInstall.exe`
7	Archivo `KMInstall.exe`

Introduzca el siguiente filtro para mostrar sólo el primer flujo: `tcp.stream eq 0`
Luego siga la conexión (botón derecho sobre cualquier paquete, Follow TCP Stream).

Conteste las siguientes preguntas:

9. ¿Cuál es la dirección IP del equipo que origina la conexión? ¿Y cuál es la dirección IP del que la recibe?
10. ¿Por cuál puerto recibe el servidor la conexión?
11. ¿Podría determinar el sistema operativo del servidor, a partir de la primera respuesta del mismo?
12. Explique qué hacen los 7 primeros comandos dados por el cliente, y cómo los contesta el servidor.
13. Explique la respuesta al octavo comando (PASV). En particular, ¿qué significan los números que van a continuación de la respuesta “Entering Passive Mode”?
14. ¿Por qué no se ve ningún listado de directorio como respuesta al comando LIST?

Ahora muestre el segundo flujo: `tcp.stream eq 1`

Y siga la conexión (botón derecho sobre cualquier paquete, Follow TCP Stream).

Conteste las siguientes preguntas:

15. ¿Cuál es la dirección IP del equipo que origina la conexión? ¿Y cuál es la dirección IP del que la recibe?
16. ¿Por cuál puerto recibe el servidor la conexión? ¿Tiene este número de puerto alguna relación con la pregunta 12?
17. ¿Qué contiene este flujo de datos? ¿Tiene esto alguna relación con la pregunta 13?

Revise ahora los flujos 2, 3, 4 y 5. Podrá comprobar que son muy parecidos a los flujos 0 y 1.

Ahora analice el flujo 6, y conteste las siguientes preguntas:

18. ¿Cuál comando se emplea para iniciar la transferencia del archivo?
19. ¿Por cuál puerto se llevará a cabo la conexión de datos? ¿Quién la recibirá?

Analice ahora el flujo 7, y conteste la siguiente pregunta:

20. ¿Cuál es la dirección IP del equipo que origina la conexión? ¿Y cuál es la dirección IP del que la recibe?
21. ¿Por cuál puerto recibe el servidor la conexión? ¿Coincide con el número que usted calculó en la pregunta 18?
22. ¿Cómo podría comprobarse que lo que está viajando por esta conexión es, en efecto, un archivo .EXE?

ANÁLISIS DE UNA SESIÓN DE FTP EN MODALIDAD ACTIVA

Cargue en Wireshark el archivo `FTP_Activo.pcapng`, que podrá encontrar en Moodle. Este archivo contiene una sesión completa del protocolo FTP, en 5 flujos TCP:

ID Flujo	Contenido
0	Solicitud del directorio raíz y el directorio /leonardo
1	Contenido del directorio raíz
2	Contenido del directorio `/leonardo`
3	Solicitud de un archivo PowerPoint
4	Archivo PowerPoint

Analice el flujo 0 del archivo, y conteste las siguientes preguntas:

23. ¿Cuál es la dirección IP del equipo que origina la conexión? ¿Y cuál es la dirección IP del que la recibe?
24. ¿Por cuál puerto recibe el servidor la conexión?
25. Explique qué hacen los 9 primeros comandos dados por el cliente, y cómo los contesta el servidor
26. Explique qué hace el décimo comando (PORT) y qué quieren decir sus parámetros.

Analice ahora el flujo 1, y conteste las siguientes preguntas:

27. ¿Cuál es la dirección IP del equipo que origina la conexión? ¿Y cuál es la dirección IP del que la recibe?
28. ¿Por cuál puerto recibe el receptor la conexión? ¿Tiene este número de puerto alguna relación con la pregunta 26? ¿Qué diferencia fundamental nota con respecto a la transferencia pasiva, que se exploró en la sección anterior?
29. ¿Qué contiene este flujo de datos?

Ahora analice el flujo 3, y conteste las siguientes preguntas:

30. ¿Cuál comando se emplea para iniciar la transferencia del archivo?
31. ¿Por cuál puerto se llevará a cabo la conexión de datos? ¿Quién la recibirá?

Analice ahora el flujo 4, y conteste la siguiente pregunta:

32. ¿Cuál es la dirección IP del equipo que origina la conexión? ¿Y cuál es la dirección IP del que la recibe?
33. ¿Por cuál puerto recibe el receptor la conexión? ¿Coincide con el número que usted calculó en la pregunta 31?
34. ¿Cómo podría comprobarse que lo que está viajando por esta conexión es, en efecto, un archivo .PPT?