TELNET Y FTP

Iker Fernández, María Fernández, Lucía Molinero, Paula Tapias, Nahia Galván y Aitzol Rivera

PROFESOR:
Roberto Olea
CURSO: 2
GRUPO: 5

ÍNDICE

1. INTRODUCCIÓN

1.1. TELNET

Telnet (*Telecommunication Network*) es un protocolo de red TCP/IP que se utiliza para acceder a un ordenador para manejarlo de forma remota. Este protocolo emplea un modelo cliente-servidor, donde el servidor recibe las solicitudes entrantes del cliente y, posteriormente, éste inicia la conexión. Por medio de dicha conexión el cliente es capaz de enviar comandos de texto en modo terminal al servidor, el cuál corresponde al dispositivo controlado.

Este protocolo se ha utilizado durante mucho tiempo por los técnicos y administradores para solucionar problemas en el dispositivo, en la red, para acceder al router, etc. Aunque por su falta de seguridad (será explicado posteriormente) fue remplazado por el protocolo SSH (Secure Shell).

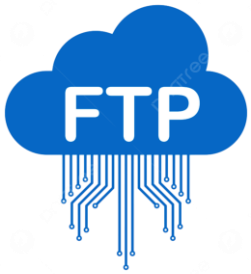
1.2. FTP

El protocolo FTP (*File Transfer Protocol*), es un protocolo para la transferencia de archivos entre un cliente (HOST) y un servidor en una red TCP. Puede ser utilizado directamente por un usuario en un terminal, pero está diseñado principalmente para ser utilizado por programas.

Este protocolo admite dos modos de transferencia de datos; el modo ASCII, utilizado para transferir archivos con caracteres imprimibles y el binario para archivos comprimidos, ejecutables.

Tiene dos modos de conexión del cliente, activo y pasivo. El pasivo surgió debido a que el activo tiene muchos problemas de seguridad ya que se acepta cualquier conexión de entrada y puede ser una amenaza si estamos en una red insegura.

Además, ha sido una herramienta clave durante mucho tiempo para cargar, descargar y gestionar archivos de forma remota. Sin embargo, debido a su falta de cifrado y vulnerabilidades de seguridad, ha sido reemplazado en muchos casos por protocolos más seguros.



2. FUNCIONAMIENTO

2.1. TELNET

1. **Inicio de la conexión.** El usuario abre un cliente Telnet y establece una conexión con el servidor remoto por medio del puerto 23.
2. **Autenticación.** Se suele solicitar una contraseña al cliente para poder acceder al sistema.
3. **Interacción.** Desde la terminal, el cliente puede ejecutar comandos (precedidos de IAC) que tendrán efecto en el servidor, como si estos comandos estuvieran siendo escritor desde el propio dispositivo/servidor.
4. **Cierre de la conexión:** La conexión se cerrará cuando el usuario así lo indique.

2.1.1. EJEMPLO

```
Cliente envía: IAC DO ECHO (Comando de control para habilitar la opción ECHO)

Servidor responde: IAC WILL ECHO (Comando de control que acepta la opción ECHO)

Cliente envía: "Hola servidor"

Servidor responde: "Hola cliente"
```

En este ejemplo, los comandos de control sirven para configurar las opciones del protocolo, mientras que los datos enviados son los mensajes de texto que el cliente y el servidor intercambian.

2.2. FTP

1. **Inicio de la conexión.** El usuario abre un cliente FTP y establece una conexión con el servidor a través del puerto 21.

    1.1 **Modo activo:** Cliente informa del puerto, el servidor inicia la conexión desde el puerto 20

    1.2 **Modo pasivo**: El cliente solicita el puerto al servidor e inicia la conexión en ese puerto dinámico especificado por el servidor.

2. **Autenticación**. Se solicita nombre y contraseña para acceder al servidor, también existen conexiones anónimas y de invitado.

3. **Interacción**. El cliente puede listar directorios, subir o descargar archivos, dependiendo del modo de transferencia se establece una segunda conexión.

4. **Cierre de la conexión**. La sesión finaliza cuando el usuario lo indica con un comando de salida, cerrando las conexiones de control y datos.

2.2.1. EJEMPLO

```
Cliente envía: USER grupo5

Servidor responde: 331 Password required for grupo5.

Cliente envía: PASS FTP

Servidor responde: 230 User grupo5 logged in.

Cliente envía: PWD

Servidor responde: 257 "/home/grupo5" is the current directory.

Cliente envía: LIST

Servidor responde: 150 Opening ASCII mode data connection for file
list.

Servidor envía datos: GRUPO5.txt

Servidor responde: 226 Transfer complete.

Cliente envía: QUIT

Servidor responde: 221 Goodbye.
```

En este ejemplo, se solicita la contraseña, una vez accedido y elegido directorio, se envían los datos, y una vez transferidos, se cierra la sesión FTP.

3. VENTAJAS Y DESVENTAJAS

3.1. TELNET

Ventajas

- Permite acceder a los dispositivos en cualquier ubicación de manera sencilla.
- No tiene un alto consumo de recursos.
- Es compatible con múltiples sistemas operativos (Windows, Linux, etc.), no es necesario que cliente y servidor tengan el mismo S.O.
- Es compatible con los estándares TCP/IP, por lo que, se puede comprobar la funcionalidad de otros servicios que también utilizan TCP/IP como protocolo de transporte.
- No requiere de una interfaz, sólo usa texto.

Desventajas

- Tiene una gran carencia de seguridad, ya que, no cifra los datos (texto plano), por lo que, resulta sencillo interceptar los comandos y contraseñas.
- En el caso de no estar bien configurado cualquiera podría acceder a la conexión.
- Ha quedado obsoleto tras la aparición del protocolo SSH, el cual tiene mayor seguridad.

3.1.1. SSH

La alternativa segura del protocolo Telnet, como ya se ha mencionado, es el protocolo SSH (Secure Shell). Aunque con las mismas características que Telnet, SSH establece la conexión por medio de un túnel cifrado que encripta los datos con estándares como AES (Advanced Encryption Standard) y Diffie-Hellman (DH) y ECDH.

Asimismo, SSH incorpora algoritmos de autenticación para comprobar la identidad del usuario y así prevenir accesos no autorizados. RSA (Rivest-Shamir-Adleman), es uno de los más empleados, se utiliza, por ejemplo, en la autenticación de claves públicas para conexiones seguras en GitHub y la gestión de repositorios en Eclipse.

3.2. FTP

Ventajas

- Agiliza los procesos de intercambio de información ya que es una transferencia directa de archivos, permite subir y descargar archivos sin ningún problema de manera bidireccional.
- Puede ser usado por cualquier sistema operativo
- Funcionamiento sencillo. No hace falta conocimiento de comandos, ni técnicos.

Desventajas

- No cifra las credenciales y los datos, es decir que puede ser un peligro en caso de la lectura de terceros
- Considerado como viejo. No es compatible con los cortafuegos modernos.
- Ralentización del proceso: no trabaja en paralelo.
- No se permite la automatización de procesos. Esto si se permite en las conexiones SSH ya mencionadas anteriormente.

4. CONCLUSIONES

4.1. TELNET

Hoy en día, Telnet ha quedado obsoleto debido a su falta de seguridad, pues transmite datos en texto plano, sin cifrar, lo que le hace vulnerable a la interceptación de información. Aunque en su momento fue una herramienta fundamental su uso ha sido reemplazado casi por completo por el más seguro protocolo SSH, ya que ofrece cifrado, autenticación y protección.

A pesar de su obsolescencia, el protocolo Telnet aún se utiliza en algunas redes privadas controladas. Sin embargo, SSH es la opción recomendada siempre que se busque seguridad.

4.2. FTP

FTP, hoy en día, no está obsoleto, pero al igual que ha ocurrido con TELNET, la falta de cifrado lo hace vulnerable y ha sido reemplazo por SFTP y FTPS. Sin embargo, sigue siendo útil en redes privadas o donde no preocupa la seguridad, ya que es muy eficaz y simple, es compatible con diversos sistemas.

Ha sido muy importante en la historia de las comunicaciones digitales, pero hoy en día, ha reducido significativamente su uso.

5. BIBLIOGRAFÍA

1. **Wikipedia**. (s.f.). **Telnet**. Obtenido de https://es.wikipedia.org/wiki/Telnet
2. **Definición de**. (s.f.). **Telnet**. Obtenido de https://definicion.de/telnet/
3. **NinjaOne**. (2021, 18 de marzo). **¿Qué es Telnet?** Obtenido de https://www.ninjaone.com/es/it-hub/it-service-management/que-es-telnet/
4. **Profesional Review**. (2019, 20 de enero). **¿Qué es Telnet?** Obtenido de https://www.profesionalreview.com/2019/01/20/telnet-que-es/
5. **IBM**. (s.f.). **Telnet Protocol**. Obtenido de https://www.ibm.com/docs/es/aix/7.1?topic=protocols-telnet-protocol
6. **Wikipedia**. **FTP**. Obtenido de https://es.wikipedia.org/wiki/Protocolo_de_transferencia_de_archivos
7. **Definición de FTP**. Obtenido de google academics https://www.rfc-editor.org/rfc/rfc354
8. **FTP PROTOCOL**. Obtenido de RFC 959. https://www.rfc-es.org/rfc/rfc0959-es.txt
9. **Modos FTP**. Obtenido de https://slacksite.com/other/ftp.html#passive