**Actividades FTP**

1. Indica con detalle motivos por los cuales conviene montar un servidor FTP en nuestra red local. ¿Y un servidor TFTP?

* Es conveniente montar un servidor FTP en nuestra red local para poder compartir y transferir archivos con los otros usuarios de la red, sin importar el sistema operativo que dispongan y almacenando estos archivos en un servidor.
* Es conveniente montar un servidor TFTP cuando es necesario realizar transferencia de archivos pequeños y de manera sencilla por lo que se usa el protocolo UDP de la capa de transporte el cual es más rápido aunque menos seguro.

1. Indica si la frase siguiente es verdadera o falsa justificando tu respuesta: “El servidor FTP en una conexión anónima requiere autenticación como usuario anonymous y contraseña una dirección de correo electrónico”.

* La frase es falsa. El servidor FTP se puede configurar para que no pida ni usuario ni contraseña a la hora de conectarse a dicho servicio.

1. ¿El cliente FTP establece una conexión de control con el servidor? ¿Por qué puerto? ¿Y el TFTP?

* Sí, el cliente y servidor establecen una conexión de control con el servidor, a través del puerto TCP 21.
* El TFTP utiliza el mismo puerto para la transferencia de datos y el control, es decir, el puerto UDP 69.

1. ¿Cuándo indica el servidor FTP al cliente, por el canal de control, el puerto al que debe conectarse el cliente? ¿Qué orden FTP cambia a este modo?

* Cuando el cliente quiere conectarse con el servidor FTP, este manda un mensaje de control al servidor el cual se recibe a través del puerto TCP 21. Una vez recibido el mensaje, el servidor contesta al cliente con el puerto que se utilizará para la conexión.
* Para cambiar el modo activo o pasivo de la conexión FTP es necesario utilizar el comando oportuno a la hora de establecer la conexión.

1. Relaciona en tu cuaderno el protocolo de transporte y su puerto de conexión con el protocolo de aplicación y su función.

FTP, datos, modo activo

FTP, datos, modo pasivo

FTP, control

TFTP, datos

TCP, 20

TCP, 21

UDP, 69

TCP, > 1024

1. ¿Un cliente FTP permite continuar una descarga en el punto en el que se quedó? ¿Y uno TFTP?

* Sí, el cliente puede interrumpir una descarga y continuar con dicha descarga una vez se vuelva a conectar al servidor.
* El cliente TFTP no puede reanudar la comunicación ya que las conexiones de se realizan de manera anónima a través del puerto UDP 69

1. ¿En modo gráfico, Windows, cómo podrías saber si el servidor FTP está activo?

* A través de la aplicación que se esté utilizando, ya sea la propia de Windows Server o una aplicación externa, es posible visualizar el estado del servidor a través de la aplicación versión servidor.

1. ¿Qué diferencia hay entre FTP y P2P?

* El protocolo FTP requiere de un servidor donde se suben y se bajan los archivos, y en este servidor se almacenan los archivos. Sin embargo, en P2P los archivos son almacenados por los usuarios y estos son los encargados de transferirse los archivos directamente.

1. Busca noticias sobre agujeros de seguridad en FTP. Haz un resumen indicando los fallos detectados y las posibles consecuencias que pueden tener en el propio servicio FTP o, de forma indirecta, en otros.

* **Noticia a)**
  + Fuente → <https://www.redeszone.net/2011/07/04/fallo-grave-de-seguridad-en-el-servidor-ftp-vsftpd-de-linux/>
  + Fecha: 4 de julio de 2011
  + Descripción: Fallo de seguridad en el servidor FTP Linux llamado “vsftpd”. Al introducir el nombre de usuario “:)” se tendrá acceso total al servidor. Cualquier usuario podrá utilizar cualquier comando del servidor y hacer un uso indebido o simplemente borrar la información. Los desarrolladores sacaron al poco tiempo una versión actualizada que corregía el fallo.
* **Noticia b)**
  + Fuente → <http://www.zonavirus.com/noticias/2019/cuidado-si-usas-proftpd-un-millon-de-servidores-ftp-afectados-por-una-grave-vulnerabilidad.asp>
  + Fecha: 23 de julio de 2019
  + Descripción: Vulnerabilidad en el servidor FTP llamado ProFTPD. A través de esta vulnerabilidad los usuarios podían “saltarse” la autenticación y ejecutar todo tipo de comandos. El fallo fue solucionado por los desarrolladores con una versión posterior.
* **Noticia c)**
  + Fuente → <https://www.muyseguridad.net/2017/02/23/fallos-java-python-saltar-firewalls-inyeccion-ftp/>
  + Fecha: 23 de febrero de 2017
  + Descripción: Java y Python no realizan ninguna comprobación en el nombre de usuario lo que puede dar lugar a inyecciones de código a través del protocolo FTP. De esta forma los atacantes se pueden saltar el firewall del servidor.

1. Busca en Internet el vídeo más ilustrativo y de mayor calidad relacionado con lo que se ha estudiado en la unidad.

* Link → <https://www.youtube.com/watch?v=flpugX8DSvQ>
* Resumen: el video explica de forma clara y concisa qué es un servidor FTP, sus funciones y las ventajas que nos aporta utilizar dicho servidor.