**TEMA 4: FTP Seguro**

**1. FTP**

El protocolo FTP es el protocolo de transferencia de archivos. Es un protocolo de la capa de aplicación que utiliza el protocolo TCP de la capa de transporte.

Utiliza una arquitectura cliente-servidor, por lo que varios clientes pueden conectarse al mismo servidor.

Para gestionar la conexión utiliza por defecto el puerto TCP 21. Para transmitir la información utiliza otros puertos. La autenticación y la transferencia de datos se realiza sin ningún tipo de cifrado.

**1.1 FTP Modo activo**

Servidor y cliente usan el puerto 21 para la conexión.

El servidor usa el puerto 20 para el canal de datos

El cliente usa un puerto aleatorio superior al 1024 para el canal de datos. Deben estar abiertos todos los puertos superiores al 1024, lo que es peligroso si estamos conectados a internet.

**1.2 FTP Modo pasivo**

Servidor y cliente usan el puerto 21 para la conexión.

El servidor usa un puerto TCP dentro de un rango disponible elegido por el administrador para el canal de datos

El cliente usará el puerto indicado por el servidor para el canal de datos.

**2. FTP Seguro**

**2.1 FTPS**

El FTPS implícito es una forma antigua de proporcionar seguridad y privacidad.

El cliente se conecta al puerto TCP 990 para la conexión y al puerto TCP 989 para los datos.

Antes de intercambiar ninguna información, se asegura el canal mediante una negociación TLS/SSL

**2.2 FTPES**

El FTPS explícito es una forma antigua de proporcionar seguridad y privacidad.

Servidor y cliente utilizan el puerto TCP 21 para la conexión

El cliente se conecta y utilizará una comunicación cifrada con TLS antes de autenticarnos y transferir información.

La información se transmite por un puerto aleatorio dentro de un rango.

Es el protocolo que se utiliza actualmente

**2.3 SFTP**

Es un nuevo protocolo basado en SSH y no en FTP, usando la criptografía del protocolo SSH para el servidor de archivos.

Usa el puerto TCP 22 por defecto y la misma forma de autenticación que SSH. Su seguridad es similar a FTPES

**2.4 AES-NI**

Es un juego de instrucciones incorporados en los procesadores Intel y AMD más recientes. Permite cifrar datos a gran velocidad en comparación con el AES tradicional.