**1. Servicio de Transferencia de Archivos (FTP)**

* **Protocolo FTP:** Permite la transferencia de archivos mediante una arquitectura cliente-servidor. Usa los puertos **21 (control)** y **20 (datos)**.
* **Tipos de acceso:**
  + **Anónimo:** Usuario “anonymous” con acceso limitado.
  + **Autorizado:** Usuarios del sistema o virtuales con permisos específicos.
* **Modos de conexión:**
  + **Activo:** El servidor inicia la conexión de datos (puede dar problemas con firewalls).
  + **Pasivo:** El cliente inicia la conexión de datos (más seguro y recomendado).
* **Tipos de transferencia:**
  + **ASCII:** Para archivos de texto.
  + **Binario:** Para archivos multimedia y ejecutables.
* **Seguridad en FTP:** No cifra los datos, vulnerable a ataques. Alternativas seguras:
  + **FTPS:** FTP con cifrado SSL/TLS.
  + **SFTP:** Basado en SSH, más seguro que FTP.

**2. Servicio TFTP**

* **Protocolo simple basado en UDP**, sin autenticación ni cifrado.
* Usado en dispositivos de red para cargar configuraciones y copias de seguridad.

**3. Servicios SFTP y SCP**

* **SFTP (Secure File Transfer Protocol):** Usa SSH, permite administrar archivos de forma segura.
* **SCP (Secure Copy Protocol):** Similar a SFTP, pero solo permite copiar archivos.
* **Ambos funcionan en el puerto 22 y garantizan autenticación, cifrado e integridad.**

**4. Transferencia de Archivos en el Despliegue Web**

* Se usa FTP, SFTP o SCP para subir archivos a servidores web.
* Los hosting permiten FTP y, en algunos casos, SFTP/SCP para mayor seguridad.
* **Errores comunes en FTP:**
  + **Access denied:** Verificar permisos.
  + **Too many connections:** Cerrar sesiones inactivas.
  + **Problemas con nombres de archivos:** En Linux, mayúsculas y minúsculas importan.

**1. ¿Qué es el servicio de acceso y control remoto?**

Permite administrar equipos de manera remota sin necesidad de acceso físico. Se utiliza para gestionar servidores, controlar servicios, transferir archivos, instalar aplicaciones, etc. Es fundamental implementar medidas de seguridad para evitar accesos no autorizados.

**2. Telnet**

* Protocolo de red que permite acceder y controlar remotamente un equipo como si estuviéramos frente a él.
* Usa el puerto 23.
* No ofrece cifrado, lo que lo hace inseguro.
* En desuso debido a sus vulnerabilidades.

**3. SSH (Secure Shell)**

* Protocolo seguro para conexiones remotas, definido en el RFC 4251.
* Desarrollado en 1995 por Tatu Ylönen.
* Usa el puerto 22 y permite autenticación por contraseña o claves.
* Cifra la comunicación evitando ataques como la interceptación de datos y el "man in the middle".
* OpenSSH es la implementación libre más utilizada.
* Existen dos versiones: SSH1 (menos segura) y SSH2 (más segura).

**4. Escritorios remotos**

* Permiten acceder a una interfaz gráfica remota.
* Se pueden securizar usando SSH.
* Ejemplos: Escritorio remoto de Windows, VNC.

**5. Protocolo VNC**

* Aplicaciones como RealVNC, UltraVNC, ThinVNC y TigerVNC permiten el acceso remoto con interfaz gráfica.
* Funciona con un servidor (VNC Server) y un cliente (VNC Viewer).
* Es multiplataforma.

**6. Servicios de Terminal Server en Windows**

* Permiten a varios usuarios conectarse simultáneamente a un servidor.
* Utiliza el protocolo RDP (Remote Desktop Protocol).
* Usa el puerto 3389.
* Facilita la ejecución de aplicaciones y control de escritorios remotos.

**7. Otros productos**

**7.1. LogMeIn**

* Permite acceso remoto rápido y seguro vía web.
* Funcionalidades: transferencia de archivos, impresión remota, escritorio compartido, Wake on LAN, seguridad con cifrado SSL de 256 bits.

**7.2. TeamViewer**

* Software de control remoto con encriptación AES de 256 bits.
* No requiere abrir puertos en routers.
* Permite asistencia y enseñanza remota.
* Transferencia de archivos rápida.
* Funciona con un ancho de banda mínimo de 128 kb/s.