📁 LPIC-2 / 🔒 Tema 212 - La seguridad del sistema

7.6.2 212.2 Administración de servidores FTP (peso: 2)

Teoría

FTP (File Transfer Protocol) es un protocolo estándar para transferir archivos entre sistemas en una red. Aunque es uno de los protocolos más antiguos y su uso ha disminuido en favor de alternativas más seguras como SFTP o SCP (basados en SSH) o protocolos web (HTTP/HTTPS), sigue siendo relevante en algunos entornos y es parte del temario de LPIC-2.

Principios de FTP:

- Utiliza dos canales de comunicación:
    - **Canal de Control:** Se establece en el puerto TCP 21. Se utiliza para enviar comandos FTP (login, listar directorios, cambiar directorio) y recibir respuestas del servidor. Permanece activo durante toda la sesión.
    - **Canal de Datos:** Se utiliza para transferir los datos de los archivos o listados de directorios. Se establece por separado del canal de control. Hay dos modos para establecer este canal:
        - **Modo Activo:** El cliente inicia la conexión en el puerto 21. El servidor responde en el puerto 21 y le dice al cliente en qué puerto (generalmente N > 1023) debe *escuchar* para la conexión de datos. Luego, el servidor *inicia* la conexión de datos desde su puerto 20 hacia el puerto N del cliente. **Problema de Firewall:** El firewall del cliente a menudo bloquea conexiones entrantes no solicitadas al puerto N.
        - **Modo Pasivo:** El cliente inicia la conexión en el puerto 21. El servidor responde en el puerto 21 y le dice al cliente que el servidor está *escuchando* para la conexión de datos en un rango de puertos (generalmente N > 1023) y le indica el puerto N. Luego, el cliente *inicia* la conexión de datos desde un puerto M (M > 1023) hacia el puerto N del servidor. **Mejor para Firewalls del Cliente:** Resuelve el problema del firewall del cliente al hacer que el cliente inicie la conexión de datos. Requiere que el firewall del servidor permita conexiones entrantes en el rango de puertos pasivos configurado.

Servidores FTP Comunes en Linux:

- **vsftpd (Very Secure FTP Daemon):** Conocido por ser simple, ligero y enfocado en la seguridad. Es uno de los más comunes en distribuciones modernas.
- **ProFTPD:** Un servidor FTP muy configurable, con muchas características y soporte para módulos. Su configuración es similar a la de Apache.
- **Pure-FTPd:** Otro servidor FTP ligero y seguro, con un enfoque en la facilidad de configuración y características de seguridad.

LPIC-2 puede cubrir conceptos generales aplicables a cualquier servidor FTP, pero la configuración práctica a menudo se centra en vsftpd o ProFTPD. Nos centraremos en **vsftpd** como ejemplo principal.

Configuración Básica de vsftpd:

1. **Instalación del Software:**
    - **Paquete:** `vsftpd` (estándar en ambas ramas Debian/Red Hat).
    - **Comando:** `sudo apt install vsftpd` o `sudo dnf install vsftpd`.
2. **Gestión del Servicio:**
    - **Nombre del Servicio:** `vsftpd.service` (estándar en ambas ramas).
    - **Comandos Systemd:** `sudo systemctl enable vsftpd`, `sudo systemctl start vsftpd`, `sudo systemctl status vsftpd`, `sudo systemctl restart vsftpd`, `sudo systemctl reload vsftpd` (para recargar configuración sin reiniciar).
3. **Archivo de Configuración:**
    - **Ubicación:** `/etc/vsftpd.conf` (ubicación estándar). Contiene la mayoría de los parámetros con formato `parametro=valor`.
4. **Directivas de Configuración Clave en `vsftpd.conf`:**
    - `anonymous_enable=YES/NO`: Habilita o deshabilita el acceso de usuario anónimo (sin autenticación, típicamente accede a un directorio público como `/var/ftp` o `/srv/ftp`). Por defecto es `YES`.
    - `local_enable=YES/NO`: Habilita o deshabilita el acceso de usuarios locales del sistema (usuarios definidos en `/etc/passwd`). Por defecto es `YES`.
    - `write_enable=YES/NO`: Si se permite escribir (subir archivos) para los usuarios locales. Requiere que los permisos del sistema de archivos subyacente también lo permitan. Por defecto es `NO` (para usuarios locales).
    - `chroot_local_user=YES/NO`: Si los usuarios locales deben ser enjaulados en sus directorios personales después del login, impidiendo que naveguen por todo el sistema de archivos. **Recomendado por seguridad si permites usuarios locales.** Requiere que el directorio personal no sea escribible por el usuario si usas ciertas configuraciones (ver documentación de vsftpd, a menudo se crea un subdirectorio como `public_html` dentro del home para las escrituras).
    - `chroot_list_enable=YES/NO`: Permite invertir el comportamiento de chroot para usuarios específicos.
    - `chroot_list_file=/etc/vsftpd.chroot_list`: Archivo que lista usuarios para `chroot_list_enable`.
    - `pasv_enable=YES/NO`: Habilita o deshabilita el modo pasivo. Por defecto es `YES`.

- `pasv_min_port=N`, `pasv_max_port=M`: Define el rango de puertos en el servidor que se utilizará para las conexiones de datos en modo pasivo (ej: `pasv_min_port=30000`, `pasv_max_port=31000`). **Crucial configurar esto y abrir estos puertos en el firewall del servidor si usas modo pasivo.**
- `listen=YES/NO`: Si vsftpd debe ejecutarse como un demonio independiente (standalone) escuchando en los puertos directamente. Por defecto `YES` para IPv4.
- `listen_ipv6=YES/NO`: Si vsftpd debe escuchar en puertos IPv6.
- `tcp_wrappers=YES/NO`: Integra vsftpd con `/etc/hosts.allow` y `/etc/hosts.deny` para control de acceso basado en IP.
- `userlist_enable=YES/NO`: Habilita el control de acceso basado en listas de usuarios.
- `userlist_deny=YES/NO`: Si `userlist_enable` es `YES`: si la lista es una lista de denegación (`YES`) o una lista de permisión (`NO`).
- `userlist_file=/etc/vsftpd.user_list`: Archivo que contiene la lista de nombres de usuario para `userlist_enable`.
- `ssl_enable=YES/NO`: Habilita el soporte SSL/TLS para cifrar las conexiones (FTPS - FTP Secure). Requiere certificados.
- `ssl_tlsv1_2=YES`, `ssl_tlsv1_3=YES`: Configurar versiones TLS.
- `rsa_cert_file=/etc/ssl/certs/vsftpd.pem`, `rsa_private_key_file=/etc/ssl/private/vsftpd.key`: Rutas a los archivos del certificado y clave privada (para FTPS).

Tipos de Usuarios FTP:

- **Usuarios Anónimos:** No requieren nombre de usuario y contraseña válidos (típicamente se usa "anonymous" como nombre de usuario y cualquier cosa como contraseña o email). Acceden a un directorio público predefinido. Riesgo de seguridad si se permite escritura.
- **Usuarios Locales:** Usuarios que existen en el sistema Linux (`/etc/passwd`). Se autentican con su nombre de usuario y contraseña de Linux (¡la contraseña se transmite en texto plano en FTP estándar!). Sus permisos se basan en los permisos del sistema de archivos subyacente y la configuración de vsftpd (ej: `write_enable`). A menudo se enjaulan (`chroot`) para limitar su acceso.
- **Usuarios Virtuales:** Usuarios gestionados *exclusivamente* por vsftpd, no existen en `/etc/passwd`. Sus credenciales se almacenan en una base de datos separada que vsftpd gestiona (ej: usando un backend como PAM con un archivo de base de datos, o un backend de base de datos real). Permiten dar acceso a FTP sin crear cuentas de sistema completas para cada usuario. **La configuración de usuarios virtuales es más compleja que el alcance básico.**

Seguridad de FTP:

- El principal riesgo de seguridad de FTP estándar es que **las credenciales se transmiten en texto plano**, haciéndolas vulnerables a la intercepción.

- **FTPS** (FTP Secure) utiliza SSL/TLS para cifrar los canales de control y datos (generalmente en el puerto 990 o negociado en el puerto 21). Es más seguro que FTP plano.
- **SFTP** y **SCP** (ambos basados en SSH) son alternativas mucho más seguras para transferir archivos, ya que todo el tráfico está cifrado y utilizan la infraestructura de autenticación de SSH. Siempre que sea posible, prefiere SFTP o SCP sobre FTP/FTPS.

Firewall:

- El firewall del servidor FTP debe permitir el tráfico entrante al puerto TCP 21 (canal de control).
- Si se usa Modo Activo, el firewall del cliente necesita permitir la conexión entrante al puerto de datos (generalmente alto, > 1023).
- Si se usa **Modo Pasivo** (el más común), el firewall del servidor necesita permitir el tráfico TCP entrante en el **rango de puertos pasivos** configurado en `vsftpd.conf` (`pasv_min_port` a `pasv_max_port`).