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

*Nota: Estos ejercicios implican instalar software y modificar archivos de configuración de red y firewall. Realízalos **SIEMPRE en una VM de prueba dedicada** con al menos otra VM para usar como cliente. Asegúrate de que tu VM tiene acceso a internet para la instalación de paquetes y de que tu firewall permite el tráfico FTP necesario. **Ten en cuenta los riesgos de seguridad del FTP estándar (texto plano) al probar. No uses credenciales reales.** Necesitarás privilegios de superusuario (`sudo`).*

Ejercicio 12.2.1: Instalando el Software del Servidor vsftpd

- **Objetivo:** Instalar el paquete del servidor vsftpd.
- **Requisitos:** Acceso a la línea de comandos. Privilegios de superusuario (`sudo`). Conexión a internet. **VM de prueba (servidor).**
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.
    2. **Instala vsftpd:** `sudo apt update && sudo apt install vsftpd` (Debian/Ubuntu) o `sudo dnf install vsftpd` (Red Hat/CentOS/Fedora).
    3. **Verifica el estado del servicio:** `systemctl status vsftpd.service`. Debería estar `active (running)`.

Ejercicio 12.2.2: Verificando Reglas de Firewall para FTP

- **Objetivo:** Asegurarse de que el firewall permite el tráfico del canal de control FTP.
- **Requisitos:** Privilegios de superusuario (`sudo`). Identificar la herramienta de firewall activa (Ej. 12.1.3 o 12.2.1). Puerto FTP (21 TCP). **VM de prueba (servidor).**
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.
    2. **Si usas `firewalld`:** Ejecuta `sudo firewall-cmd --zone=<zona> --list-services` o `sudo firewall-cmd --zone=<zona> --list-ports`. Busca el servicio `ftp` o el puerto `21/tcp`. Si no está en la zona relevante para la interfaz de escucha de vsftpd, añádelo: `sudo firewall-cmd --zone=<zona_interfaz> --add-service=ftp --permanent` y `sudo firewall-cmd --reload`.
    3. **Si usas `ufw`:** Ejecuta `sudo ufw status`. Busca reglas para el puerto 21 TCP. Si no están, añádelas: `sudo ufw allow 21/tcp` o `sudo ufw allow ftp`.
    4. **Si usas `iptables` directamente:** Ejecuta `sudo iptables -L -v -n`. Busca reglas que permitan el tráfico TCP entrante al puerto 21.

Ejercicio 12.2.3: Localizando y Explorando el Archivo de Configuración Principal de vsftpd

- **Objetivo:** Encontrar y ver el contenido de `vsftpd.conf`.
- **Requisitos:** vsftpd instalado. Acceso a la línea de comandos. Privilegios de superusuario (`sudo`). **VM de prueba (servidor).**
- **Desarrollo Paso a Paso:**

1. Abre una terminal.
2. **Localiza el archivo:** `/etc/vsftpd.conf`.
3. **Crea una copia de seguridad:** `sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.orig`.
4. **Visualiza el contenido:** Ejecuta `sudo less /etc/vsftpd.conf`. Observa las directivas comentadas y los valores por defecto.

Ejercicio 12.2.4: (Conceptual) Configurando Acceso Anónimo Básico

- **Objetivo:** Entender cómo habilitar el acceso sin autenticación.
- *Requisitos:* Privilegios de superusuario (`sudo`). `vsftpd.conf`. Directorio de usuario anónimo (ej: `/var/ftp`). **VM de prueba (servidor).**
- **Desarrollo Paso a Paso (Conceptual):**
  1. Abre una terminal.
  2. **Edita `vsftpd.conf`:** Ejecuta `sudo vi /etc/vsftpd.conf`.
  3. **Asegúrate de que la directiva está configurada:** `anonymous_enable=YES`.
  4. **Asegúrate de que el directorio de usuario anónimo existe y tiene permisos de lectura para "otros":** El directorio por defecto es `/var/ftp` o `/srv/ftp`. Ejecuta `ls -ld /var/ftp` y `ls -l /var/ftp/*`. Debe ser legible por el usuario "ftp" o el usuario bajo el que corre vsftpd anónimo.
  5. **Guarda y sal.**
  6. **Recarga vsftpd:** `sudo systemctl reload vsftpd`.
  7. **(Para probar):** Desde una VM cliente, usa el comando `ftp <IP_servidor>`. Como nombre de usuario, usa `anonymous`. Como contraseña, cualquier cosa (o tu email). Intenta navegar (`ls`, `cd`).

Ejercicio 12.2.5: (Conceptual) Configurando Acceso de Usuario Local Enjaulado

- **Objetivo:** Permitir a los usuarios del sistema iniciar sesión y restringirlos a su directorio personal.
- *Requisitos:* Privilegios de superusuario (`sudo`). `vsftpd.conf`. Un usuario de Linux existente. **VM de prueba (servidor).**
- **Desarrollo Paso a Paso (Conceptual):**
  1. Abre una terminal.
  2. **Edita `vsftpd.conf`:** Ejecuta `sudo vi /etc/vsftpd.conf`.
  3. **Asegúrate de que las directivas están configuradas:**
     - `local_enable=YES`
     - `write_enable=YES` (Si quieres permitir subir archivos)
     - `chroot_local_user=YES` (Para enjaular usuarios locales en su home)
  4. **Considera la configuración de `chroot_local_user` y permisos de home:** Si `chroot_local_user=YES`, el directorio home del usuario NO DEBE SER ESCRIBIBLE por el usuario de FTP por defecto para evitar un posible escape de chroot (vsftpd puede negarse a iniciar sesión si el home es escribible). Una solución

común es crear un subdirectorio dentro del home (ej: `~/ftp_upload`) y configurar vsftpd para permitir la escritura solo en ese subdirectorio, o cambiar los permisos del home a 555 y crear un subdirectorio 755 para escritura.

5. **Guarda y sal.**
6. **Recarga vsftpd:** `sudo systemctl reload vsftpd`.
7. **(Para probar):** Desde una VM cliente, usa el comando `ftp <IP_servidor>`. Usa el nombre de usuario y contraseña de un usuario de Linux existente en el servidor. Una vez logueado, intenta navegar (`ls`, `cd ..`). Si el enjaulamiento funciona, no podrás ir más allá de tu directorio home (o el subdirectorio configurado). Intenta subir un archivo si `write_enable=YES`.

Ejercicio 12.2.6: (Conceptual) Configurando Modo Pasivo y Puertos del Firewall

- **Objetivo:** Configurar vsftpd para usar un rango de puertos pasivos y abrir esos puertos en el firewall.
- *Requisitos:* Privilegios de superusuario (`sudo`). `vsftpd.conf`. Herramienta de firewall configurada. **VM de prueba (servidor).**
- **Desarrollo Paso a Paso (Conceptual):**
    1. Abre una terminal en el servidor.
    2. **Edita `vsftpd.conf`:** Ejecuta `sudo vi /etc/vsftpd.conf`.
    3. **Asegúrate de que el modo pasivo está habilitado y configura el rango de puertos:**

        ```
        pasv_enable=YES
        pasv_min_port=30000
        pasv_max_port=31000
        ```

        - Elige un rango de puertos suficiente (ej: 100-200 puertos).
    4. **Guarda y sal.**
    5. **Recarga vsftpd:** `sudo systemctl reload vsftpd`.
    6. **Configura el firewall para permitir tráfico TCP entrante en el rango de puertos pasivos:**
        - **Con `firewalld`:** `sudo firewall-cmd --zone=<zona_interfaz> --add-port=30000-31000/tcp --permanent` y `sudo firewall-cmd --reload`.
        - **Con `ufw`:** `sudo ufw allow 30000:31000/tcp`.
        - **Con `iptables`:** `sudo iptables -A INPUT -p tcp --dport 30000:31000 -m state --state NEW,ESTABLISHED -j ACCEPT`. Guarda las reglas.
    7. **(Para probar):** Desde una VM cliente, usa un cliente FTP gráfico (ej: FileZilla) o de línea de comandos que soporte modo pasivo. Conéctate al servidor FTP y realiza una transferencia de archivo. Monitoriza los logs del firewall en el servidor para ver si se permiten las conexiones en el rango de puertos pasivos.