📁 LPIC-2 / 📨 Examen 211 - Servicios de Correo Electrónico - Ejercicios

*Nota: Estos ejercicios implican instalar software y modificar archivos de configuración de red. Realízalos **SIEMPRE en una VM de prueba dedicada**. Asegúrate de que tu VM tiene acceso a internet para la instalación de paquetes y de que tu firewall permite tráfico TCP en el puerto 25 según sea necesario (entrada/salida). Necesitarás privilegios de superusuario (`sudo`).*

Ejercicio 11.2.1: Instalando Postfix (o Verificando MTA por Defecto)

- **Objetivo:** Asegurarse de que Postfix (o el MTA por defecto) está instalado.
- **Requisitos:** Acceso a la línea de comandos. Privilegios de superusuario (`sudo`). Conexión a internet.
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.
    2. **Verifica si Postfix está instalado:** Ejecuta `dpkg -l postfix` (Debian) o `rpm -q postfix` (Red Hat).
    3. **Si no está instalado o quieres asegurarte de que es el MTA por defecto:** Instálalo. Durante la instalación, selecciona el tipo "Internet Site" y proporciona el FQDN de tu VM como "System mail name" (ej: `server.mytest.local`).
        - `sudo apt update && sudo apt install postfix` (Debian)
        - `sudo dnf install postfix` (Red Hat)
    4. **Si prefieres trabajar con el MTA que tu distribución trajo por defecto (si no es Postfix), identifícalo** (Ej. 11.1.1) y adapta los pasos siguientes a su configuración (las ubicaciones de `main.cf`/`master.cf` y la sintaxis serán diferentes, pero el concepto de directivas clave es similar). **Sin embargo, LPIC-2 tiende a centrarse en Postfix.**

Ejercicio 11.2.2: Gestión del Servicio Postfix

- **Objetivo:** Asegurarse de que el servicio Postfix está corriendo y habilitado.
- **Requisitos:** Postfix instalado. Privilegios de superusuario (`sudo`).
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.
    2. **Habilita el servicio:** `sudo systemctl enable postfix`.
    3. **Inicia el servicio:** `sudo systemctl start postfix`.
    4. **Verifica el estado:** `systemctl status postfix.service`. Debería estar `active (running)`.

Ejercicio 11.2.3: Verificando Reglas de Firewall para el Puerto 25

- **Objetivo:** Asegurarse de que el firewall permite el tráfico SMTP.
- **Requisitos:** Privilegios de superusuario (`sudo`). Identificar la herramienta de firewall activa (Ej. 5.2.5). Puerto SMTP (25 TCP).
- **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 `smtp` o el puerto `25/tcp`. Si no está en la zona relevante para la interfaz donde Postfix escucha, añádelo: `sudo firewall-cmd --zone=<zona_interfaz> --add-service=smtp --permanent` y `sudo firewall-cmd --reload`.
3. **Si usas `ufw`:** Ejecuta `sudo ufw status`. Busca reglas para el puerto 25 TCP. Si no están, añádelas: `sudo ufw allow 25/tcp`.
4. **Si usas `iptables` directamente:** Ejecuta `sudo iptables -L -v -n`. Busca reglas para el tráfico TCP entrante/saliente en el puerto 25.

Ejercicio 11.2.4: Localizando y Explorando el Archivo de Configuración Principal de Postfix

- **Objetivo:** Encontrar y entender las directivas clave en `main.cf`.
- **Requisitos:** Postfix instalado. Privilegios de superusuario (`sudo`).
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.
    2. **Localiza el archivo:** `/etc/postfix/main.cf`.
    3. **Visualiza el contenido:** Ejecuta `sudo less /etc/postfix/main.cf`. Observa el formato `parametro = valor` y los comentarios.
    4. **Busca las directivas clave:** `myhostname`, `mydomain`, `myorigin`, `inet_interfaces`, `mydestination`, `mynetworks`, `relayhost`. Anota sus valores actuales.

Ejercicio 11.2.5: (Conceptual) Configurando Directivas Clave en `main.cf`

- **Objetivo:** Entender cómo modificar la configuración básica de Postfix.
- *Requisitos:* Privilegios de superusuario (`sudo`). Postfix instalado. **VM de prueba.**
- **Desarrollo Paso a Paso (Conceptual):**
    1. Abre una terminal.
    2. **Edita el archivo `main.cf`:** Ejecuta `sudo vi /etc/postfix/main.cf`.
    3. **Ajusta las directivas:**
        - `myhostname`: Asegúrate de que es el FQDN correcto de tu servidor (ej: `server.mytest.local`).
        - `mydestination`: Añade otros nombres de dominio para los que este servidor es el destino final si es necesario (separa por comas).
        - `inet_interfaces`: Cámbialo de `all` a `localhost` si solo quieres manejar correo local y enviar externo (sin recibir de otros MTAs). Cámbialo a una IP específica si solo debe escuchar allí.
        - `mynetworks`: **No añadas redes aquí a menos que sepas EXACTAMENTE lo que haces.** Mantén `127.0.0.0/8` para localhost.

    - `relayhost`: Si necesitas un relé, descomenta o añade esta línea y especifica el servidor relé (ej: `relayhost = smtp.misma-red.local` o `relayhost = [smtp.gmail.com]:587`).
4. **Guarda y sal.**
5. **Verifica la configuración:** Ejecuta `sudo postfix check`.
6. **Recarga la configuración:** Ejecuta `sudo systemctl reload postfix`.

Ejercicio 11.2.6: Enviando un Correo de Prueba y Verificando la Cola

- **Objetivo:** Enviar un correo y usar las herramientas de cola para ver su estado.
- **Requisitos:** Postfix configurado y corriendo. Comando `mail` o `mailx` instalado.
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.
    2. **Envía un correo de prueba a un usuario local:** Ejecuta `echo "Este es un correo local." | mail -s "Prueba Local" <tu_usuario_local>`.
    3. **Verifica el buzón local:** Ejecuta `mail` (sin argumentos) como el usuario de destino. Deberías ver el correo.
    4. **Envía un correo de prueba a una dirección externa (si la configuración y el firewall lo permiten):** Ejecuta `echo "Este es un correo externo." | mail -s "Prueba Externa" <tu_correo_externo@example.com>`.
    5. **Verifica la cola de correo:** Ejecuta `mailq` o `postqueue -p`. Deberías ver el mensaje que acabas de enviar (con estado `sent` si ya salió, o `queued`/`deferred` si aún está en la cola esperando para ser enviado o reintentado).
    6. **Fuerza el procesamiento de la cola (si el correo externo está en diferido):** Ejecuta `sudo postqueue -f`. Vuelve a verificar `mailq` para ver si salió.

Ejercicio 11.2.7: Verificando Logs del MTA

- **Objetivo:** Localizar y ver los logs de Postfix para diagnosticar problemas.
- **Requisitos:** Postfix corriendo. Logs generados (Ej. 11.2.6). Privilegios de superusuario (`sudo`).
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.
    2. **Localiza el archivo de log (Diferencias):** `/var/log/mail.log` (Debian/Ubuntu) o `/var/log/maillog` (Red Hat/CentOS/Fedora).
    3. **Visualiza las últimas líneas:** Ejecuta `sudo tail <ruta_log_correo>`. Busca líneas que contengan `postfix/smtp` (para envíos externos), `postfix/local` (para entregas locales), `postfix/smtpd` (para correos recibidos).
    4. **Si usas systemd, usa journalctl:** Ejecuta `journalctl -u postfix.service -f`. Mientras se ejecuta, envía un correo de prueba y observa los logs en tiempo real. Busca mensajes que indiquen si la entrega fue exitosa (ej:

`status=sent`, `status=delivered`) o si hubo errores (ej: `status=deferred`, `Connection refused`, `Name or service not known`).