📁 LPIC-2 / 🔒 Examen 212 - Seguridad del Sistema - Ejercicios

*Nota: Estos ejercicios implican modificar la configuración de red y firewall que puede afectar la conectividad. Realízalos **SIEMPRE en una VM de prueba dedicada** con múltiples interfaces de red configuradas (simulando diferentes redes). Necesitarás privilegios de superusuario (`sudo`).*

Ejercicio 12.1.1: Verificando y Habilitando el Reenvío de IP

- **Objetivo:** Asegurarse de que el kernel está configurado para reenviar paquetes.
- **Requisitos:** Acceso a la línea de comandos. Privilegios de superusuario (`sudo`).
- **Desarrollo Paso a Paso:**
  1. Abre una terminal.
  2. **Verifica el estado actual:** Ejecuta `cat /proc/sys/net/ipv4/ip_forward` o `sysctl net.ipv4.ip_forward`. Anota el valor (0 o 1).
  3. **Si el valor es 0 (deshabilitado):**
     - **Habilita temporalmente:** Ejecuta `sudo sysctl net.ipv4.ip_forward=1`. Vuelve a verificar con `sysctl`.
     - **Habilita persistentemente:** Edita `/etc/sysctl.conf` o añade un archivo en `/etc/sysctl.d/` (ej: `sudo vi /etc/sysctl.d/99-ip-forward.conf`) y añade la línea `net.ipv4.ip_forward = 1`.
     - **Aplica los cambios persistentes (sin reiniciar):** Ejecuta `sudo sysctl -p`.
  4. **Verifica el estado para IPv6 (opcional):** Ejecuta `sysctl net.ipv6.conf.all.forwarding`. Habilita si es necesario.

Ejercicio 12.1.2: Viendo la Tabla de Enrutamiento

- **Objetivo:** Examinar cómo el kernel decide por dónde enviar los paquetes.
- **Requisitos:** Acceso a la línea de comandos. Múltiples interfaces de red configuradas (Ej. 205.1).
- **Desarrollo Paso a Paso:**
  1. Abre una terminal.
  2. **Visualiza la tabla de enrutamiento principal:** Ejecuta `ip route show` o `route -n`.
  3. **Identifica las entradas clave:**
     - Rutas a redes locales conectadas a tus interfaces (ej: `192.168.1.0/24 dev eth0`).
     - La ruta por defecto (`default` o `0.0.0.0`).
  4. **Verifica si la tabla parece correcta** para la topología de red de tu VM.

Ejercicio 12.1.3: (Conceptual) Configurando NAT (Masquerading)

- **Objetivo:** Entender cómo permitir a una red privada acceder a otra red (ej: Internet) a través de la IP del router Linux.

- *Requisitos:* Privilegios de superusuario (`sudo`). Una interfaz conectada a la red privada y otra a la red de "salida". Herramienta de firewall configurada. **VM de prueba.**
- **Desarrollo Paso a Paso (Conceptual):**
    - **Con `iptables`:**
        1. Asegúrate de que el reenvío de IP está habilitado.
        2. Identifica la interfaz conectada a la red de "salida" (ej: `eth1`).
        3. Añade la regla MASQUERADE (requiere sudo): `sudo iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE`.
        4. Guarda las reglas de iptables para que persistan (el método varía por distribución, ej: `sudo service iptables save` o `sudo netfilter-persistent save`).
    - **Con `firewalld`:**
        1. Asegúrate de que el reenvío de IP está habilitado (firewalld puede manejar esto si está bien integrado con sysctl).
        2. Identifica la zona asociada a la interfaz conectada a la red de "salida" (ej: `external`).
        3. Habilita el masquerading en esa zona (requiere sudo): `sudo firewall-cmd --zone=external --add-masquerade --permanent`.
        4. Recarga firewalld: `sudo firewall-cmd --reload`.
    - **Con `ufw`:**
        1. Asegúrate de que el reenvío de IP está habilitado.
        2. Edita el archivo de reglas "before.rules" (`/etc/ufw/before.rules`) y añade reglas POSTROUTING en la tabla `nat` (proceso más manual).
        3. Edita `/etc/default/ufw` y configura el reenvío por defecto.
        4. Recarga ufw: `sudo ufw reload`.
    - **(Para probar):** Configura una VM cliente en la red privada para usar la IP de la interfaz interna del router Linux como su gateway. Intenta acceder a un recurso en la red de "salida".

Ejercicio 12.1.4: Configurando Reglas Básicas de Reenvío en Firewall (FORWARD chain)

- **Objetivo:** Permitir que el tráfico pase a través del router.
- **Requisitos:** Privilegios de superusuario (`sudo`). Herramienta de firewall configurada. Reenvío de IP habilitado. **VM de prueba.**
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.
    2. **Con `iptables`:**
        - **Lista las reglas actuales de la cadena FORWARD:** Ejecuta `sudo iptables -L FORWARD -v -n`. La política por defecto suele ser `DROP` o `REJECT`.
        - **Añade una regla básica para PERMITIR todo el reenvío (¡Solo para pruebas, NO seguro en producción!):** Ejecuta `sudo iptables -A`

`FORWARD -j ACCEPT`. (En producción, restringirías por interfaz, protocolo, puertos, IPs, etc.).
- **Guarda las reglas para que persistan.**

3. **Con `firewalld`:**
   - El reenvío entre zonas se gestiona por defecto si las zonas están configuradas correctamente. Puedes añadir reglas de reenvío de puertos o servicios específicas si es necesario (`sudo firewall-cmd --zone=<zona1> --add-forward-port=...`).
4. **Con `ufw`:**
   - UFW gestiona las reglas FORWARD automáticamente si está configurado como router. Las reglas `allow` se aplican a la cadena FORWARD por defecto.

Ejercicio 12.1.5: (Conceptual) Instalando un Demonio de Enrutamiento Dinámico

- **Objetivo:** Identificar el software para enrutamiento dinámico y sus archivos de configuración.
- *Requisitos:* Acceso a la línea de comandos. Privilegios de superusuario (`sudo`). Conexión a internet. **VM de prueba.**
- **Desarrollo Paso a Paso (Conceptual):**
  1. Abre una terminal.
  2. **Instala el paquete (elige uno):** `sudo apt install quagga` (Debian/Ubuntu) o `sudo dnf install frr` (Red Hat/CentOS/Fedora).
  3. **Verifica el estado del servicio principal:** `systemctl status quagga` o `systemctl status frr`. Debería estar instalado pero probablemente inactivo hasta que se configure.
  4. **Explora el directorio de configuración:**
     - Quagga: `ls -l /etc/quagga/`. Busca archivos como `zebra.conf`, `ripd.conf`, `ospfd.conf`.
     - FRR: `ls -l /etc/frr/`. Busca archivos similares.
  5. **Identifica la utilidad de línea de comandos VTY (si existe):** `vtysh` en Quagga, `vtysh` en FRR. Permite interactuar con los demonios de enrutamiento en tiempo de ejecución.
  6. **(Contexto):** Configurar RIP, OSPF o BGP implica editar estos archivos `.conf` o usar `vtysh` para definir las interfaces que participan, los vecinos, las redes a anunciar, etc. Luego, habilitar y arrancar los demonios específicos (ej: `ripd`, `ospfd`) además de `zebra`/`frr`.