📁 LPIC-2 / 🌐 Examen 205 - Configuración de Red - Ejercicios

Nota: Estos ejercicios implican usar herramientas de diagnóstico. Se recomienda realizarlos en una VM con acceso a internet para probar hosts remotos. Algunos requieren privilegios de superusuario (`sudo`).

Ejercicio 5.3.1: Usando `ping` para Diagnóstico Avanzado

- **Objetivo:** Usar opciones de `ping` y analizar su salida.
- **Requisitos:** Acceso a la línea de comandos.
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.
    2. **Haz ping continuo a un host remoto y observa la latencia y pérdida:** Ejecuta `ping google.com`. Presiona `Ctrl+C` después de un tiempo. Observa las estadísticas finales (pérdida de paquetes %, min/avg/max latencia).
    3. **Especifica el número de paquetes:** Ejecuta `ping -c 5 google.com`. Solo enviará 5 paquetes.
    4. **Especifica la interfaz de origen (si tienes varias):** Ejecuta `ping -I <nombre_interfaz> 8.8.8.8`. Esto es útil para asegurar que el tráfico sale por la interfaz esperada.
    5. **Haz ping a tu gateway y compáralo con un host remoto:** Ejecuta `ping <ip_gateway>`. Compara la latencia con la de `ping google.com`. La latencia al gateway debe ser muy baja. Una latencia alta al gateway puede indicar problemas en tu red local o en el router.

Ejercicio 5.3.2: Diagnosticando la Ruta con `traceroute` / `mtr`

- **Objetivo:** Identificar dónde puede estar fallando la conexión o haber un cuello de botella en la ruta.
- **Requisitos:** Acceso a la línea de comandos. `traceroute` o `mtr` instalados.
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.
    2. **Rastrea la ruta a un host remoto:** Ejecuta `traceroute google.com`. Observa cada salto. ¿Hay asteriscos o aumentos significativos de latencia en algún punto?
    3. **Usa `mtr` para un diagnóstico continuo:** Ejecuta `mtr google.com`. Observa la pérdida de paquetes y la latencia promedio para cada salto en tiempo real. Si la pérdida o latencia aumenta en un salto y se mantiene alta en los subsiguientes, el problema está en ese salto. Presiona `q` para salir.

Ejercicio 5.3.3: Probando Conectividad de Puerto con `nc`

- **Objetivo:** Verificar si servicios específicos son accesibles en sus puertos estándar.
- **Requisitos:** Acceso a la línea de comandos. `netcat` instalado.
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.

2. **Prueba el puerto SSH (22) en un host remoto (ej: un servidor al que tengas acceso):** Ejecuta `nc -zv <ip_servidor> 22`. Debería decir "Connection to ... 22 port [tcp/ssh] succeeded!" si el servicio SSH está corriendo y es accesible.
3. **Prueba el puerto HTTP (80) en un servidor web (ej: https://www.google.com/url?sa=E&source=gmail&q=google.com):** Ejecuta `nc -zv google.com 80`.
4. **Prueba el puerto HTTPS (443):** Ejecuta `nc -zv google.com 443`.
5. **Prueba un puerto que sepas que está cerrado:** Ejecuta `nc -zv google.com 1`. Debería fallar rápidamente. Esto ayuda a distinguir entre un puerto cerrado y un host inaccesible.

Ejercicio 5.3.4: Analizando Tráfico Específico con `tcpdump` y Filtros

- **Objetivo:** Aislar el tráfico relevante para un problema usando filtros.
- **Requisitos:** Privilegios de superusuario (`sudo`). `tcpdump` instalado. Un escenario para generar tráfico (ej: intentar SSH a un servidor, acceder a una página web).
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.
    2. **Identifica tu interfaz:** `ip addr show`.
    3. **Intenta hacer SSH a un servidor (en otra terminal) que sabes que está arriba pero no responde o falla de forma extraña.**
    4. **Mientras intentas SSH, captura solo el tráfico SSH para el host de destino (en la primera terminal):** Ejecuta `sudo tcpdump -i <tu_interfaz> -nnvvS host <ip_servidor> and tcp port 22`.
    5. **Analiza la salida de `tcpdump`:** ¿Ves paquetes SYN saliendo de tu máquina? ¿Ves alguna respuesta (SYN/ACK, RST, o nada)? Si ves SYN saliendo pero nada volviendo, el problema está en el servidor, el firewall entre tú y el servidor, o la ruta de retorno. Si ves SYN saliendo y RST volviendo, el puerto está cerrado en el servidor. Si no ves SYN saliendo, el problema está en tu máquina (configuración IP, routing, firewall local).
    6. **Captura tráfico DNS (si sospechas de DNS):** Ejecuta `sudo tcpdump -i <tu_interfaz> -nnvvS udp port 53`. Mientras se ejecuta, haz `host <hostname>` o `ping <hostname>`. Deberías ver las consultas DNS saliendo a tus servidores DNS configurados y las respuestas volviendo.
    7. **Detén `tcpdump`:** `Ctrl+C`.

Ejercicio 5.3.5: Verificando Servicios y Puertos a la Escucha

- **Objetivo:** Asegurarse de que un servicio de red está corriendo y escuchando en el puerto correcto.
- **Requisitos:** Acceso a la línea de comandos. Privilegios de superusuario (`sudo`) para ver nombres de procesos.
- **Desarrollo Paso a Paso:**

1. Abre una terminal.
2. **Lista los puertos TCP a la escucha y los procesos:** Ejecuta `sudo ss -tulnp`. Busca la línea para el servicio que esperas (ej: `tcp LISTEN 0 128 *:22 users:(("sshd",pid=XXX,fd=Y))`). Verifica el puerto y la dirección (`*` significa todas las IPs, `127.0.0.1` significa solo localhost).
3. **Lista los puertos UDP a la escucha:** Ejecuta `sudo ss -u lnp`. (Ej: Puerto 53 para DNS si `systemd-resolved` o un servidor DNS está corriendo).
4. **Verifica el estado del servicio con `systemctl`:** Ejecuta `systemctl status ssh.service` (o `sshd.service`, `apache2.service`, `httpd.service`, etc.). Asegúrate de que está `active (running)`. Si falla, revisa sus logs (`journalctl -u <nombre_servicio>`).

Ejercicio 5.3.6: (Conceptual) Depurando un Problema de Enrutamiento Temporal

- **Objetivo:** Usar comandos de enrutamiento para diagnosticar un fallo temporal.
- **Escenario Hipotético:** Accidentalmente borraste la ruta por defecto o añadiste una ruta incorrecta y perdiste conectividad externa.
- **Requisitos:** Acceso a la línea de comandos. Privilegios de superusuario (`sudo`). **VM de prueba.**
- **Desarrollo Paso a Paso (Simulado):**
  1. Abre una terminal.
  2. **Verifica la tabla de enrutamiento:** Ejecuta `ip route show`. Nota la línea `default`.
  3. **(Simula borrar la ruta por defecto - NO EJECUTAR a menos que estés seguro):** `sudo ip route del default`. Perderías conectividad externa.
  4. **Intenta hacer ping a un host remoto:** Fallará.
  5. **Verifica la tabla de enrutamiento de nuevo:** Ejecuta `ip route show`. La ruta por defecto ya no está.
  6. **Añade la ruta por defecto de vuelta:** Ejecuta `sudo ip route add default via <ip_gateway> [dev <tu_interfaz>]`.
  7. **Verifica la tabla de enrutamiento:** La ruta por defecto debería estar de vuelta.
  8. **Haz ping a un host remoto:** Debería funcionar de nuevo.
  9. **(Recordatorio):** Los cambios hechos con `ip route add/del` son temporales. La configuración persistente se gestiona en los archivos/herramientas vistos en 205.1.