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

*Nota: Estos ejercicios implican modificar la configuración del firewall que puede bloquear el acceso remoto (SSH). Realízalos **SIEMPRE en una VM de prueba dedicada**. Mantén una sesión de consola directa (no SSH) o un snapshot de la VM antes de hacer cambios que puedan bloquearte. Necesitarás privilegios de superusuario (`sudo`). Identifica qué herramienta de firewall usa tu VM por defecto.*

Ejercicio 12.2.1: Identificando la Herramienta de Firewall Activa

- **Objetivo:** Determinar qué software de gestión de firewall está en uso en el sistema.
- **Requisitos:** Acceso a la línea de comandos. Privilegios de superusuario (`sudo`).
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.
    2. **Verifica el estado de los servicios comunes:** Ejecuta `systemctl status firewalld ufw iptables`. Uno o más podrían estar activos. Firewalld y ufw son servicios de alto nivel. `iptables` sin un servicio de persistencia simplemente ejecuta las reglas en memoria (verifica si hay un servicio como `netfilter-persistent` o `iptables-persistent`).
    3. **Comprueba la existencia de comandos:** Ejecuta `which firewall-cmd`, `which ufw`, `which iptables`. Esto te dice qué herramientas están instaladas.
    4. **Conclusión:** Basado en los servicios activos y los comandos disponibles, determina la herramienta principal en uso (ej: si `firewalld` está activo y `ufw` inactivo, probablemente usa firewalld).

Ejercicio 12.2.2: (Conceptual) Listando Reglas de Firewall con `iptables`

- **Objetivo:** Entender la salida del comando `iptables -L`.
- *Requisitos:* Comprensión básica de `iptables`. Acceso a la línea de comandos.
- **Desarrollo Paso a Paso (Conceptual):**
    1. Abre una terminal.
    2. **Visualiza las reglas de la tabla `filter` (la más común):** Ejecuta `sudo iptables -L -v -n`.
        - `-L`: Lista reglas.
        - `-v`: Verbose (muestra contadores de paquetes/bytes).
        - `-n`: Numérico (no intenta resolver IPs/puertos a nombres).
    3. **Observa la salida:** Verás las cadenas `INPUT`, `FORWARD`, `OUTPUT` con sus políticas por defecto (`policy`). Debajo de cada cadena, verás la lista de reglas. Cada regla tiene columnas para el target (`target`), protocolo (`prot`), opt, origen (`source`), destino (`destination`), y las condiciones (`<match>`).
    4. **Visualiza reglas de la tabla `nat`:** Ejecuta `sudo iptables -t nat -L -v -n`. Observa las cadenas `PREROUTING`, `INPUT`, `OUTPUT`, `POSTROUTING`. Aquí verás reglas de NAT/Masquerading.

Ejercicio 12.2.3: (Conceptual) Gestionando Firewall con `firewall-cmd`

- **Objetivo:** Entender cómo listar y gestionar la configuración con `firewalld`.
- *Requisitos:* `firewalld` instalado y corriendo. Acceso a la línea de comandos.
- **Desarrollo Paso a Paso (Conceptual):**
    1. Abre una terminal.
    2. **Verifica el estado de firewalld:** Ejecuta `sudo firewall-cmd --state`.
    3. **Lista todas las configuraciones (zonas, interfaces, servicios, puertos, etc.):** Ejecuta `sudo firewall-cmd --list-all`.
    4. **Lista la configuración de una zona específica (ej: `public`):** Ejecuta `sudo firewall-cmd --zone=public --list-all`.
    5. **Añade un servicio (ej: http) temporalmente a una zona:** `sudo firewall-cmd --zone=public --add-service=http`. Prueba a acceder al servicio.
    6. **Elimina el servicio temporal:** `sudo firewall-cmd --zone=public --remove-service=http`.
    7. **Añade un servicio permanentemente a una zona:** `sudo firewall-cmd --zone=public --add-service=http --permanent`.
    8. **Aplica los cambios permanentes:** `sudo firewall-cmd --reload`.
    9. **Lista los servicios permanentes de una zona:** `sudo firewall-cmd --zone=public --list-services --permanent`.

Ejercicio 12.2.4: (Conceptual) Gestionando Firewall con `ufw`

- **Objetivo:** Entender cómo listar y gestionar la configuración con `ufw`.
- *Requisitos:* `ufw` instalado y corriendo. Acceso a la línea de comandos.
- **Desarrollo Paso a Paso (Conceptual):**
    1. Abre una terminal.
    2. **Verifica el estado de ufw:** Ejecuta `sudo ufw status`. Si está inactivo, habilítalo (¡asegúrate de que la regla para SSH está permitida si estás conectado por SSH!): `sudo ufw enable`.
    3. **Lista las reglas (más detallado):** Ejecuta `sudo ufw status verbose`.
    4. **Permitir tráfico entrante a un puerto (ej: 80 TCP):** `sudo ufw allow 80/tcp`.
    5. **Denegar tráfico entrante a un puerto (ej: 25 TCP):** `sudo ufw deny 25/tcp`.
    6. **Permitir tráfico entrante desde una IP a un puerto:** `sudo ufw allow from 192.168.1.10 to any port 22`.
    7. **Eliminar una regla:** `sudo ufw delete allow 80/tcp`.
    8. **Recargar reglas:** `sudo ufw reload`.

Ejercicio 12.2.5: (Conceptual) Configurando una Regla de Firewall (Ej: Permitir SSH)

- **Objetivo:** Permitir conexiones SSH entrantes.

- *Requisitos:* Privilegios de superusuario (`sudo`). Herramienta de firewall activa. Puerto SSH (22 TCP). **VM de prueba. Mantén sesión de consola.**
- **Desarrollo Paso a Paso (Conceptual):**
    - **Con `iptables`:** Asegúrate de que la política de `INPUT` no sea `ACCEPT`. Añade la regla *antes* de cualquier regla de `DROP`/`REJECT` general para la cadena `INPUT`: `sudo iptables -A INPUT -p tcp --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT`. Asegúrate de que también permites el tráfico establecido/relacionado (`sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT`). Guarda las reglas persistentes.
    - **Con `firewalld`:** Identifica la zona de la interfaz donde esperas conexiones SSH entrantes. Añade el servicio ssh a esa zona: `sudo firewall-cmd --zone=<zona> --add-service=ssh --permanent` y `sudo firewall-cmd --reload`.
    - **Con `ufw`:** Asegúrate de que ufw está habilitado. Añade la regla para permitir el servicio ssh: `sudo ufw allow ssh`. Si ssh no es reconocido como servicio, usa el puerto: `sudo ufw allow 22/tcp`.

Ejercicio 12.2.6: (Conceptual) Verificando Logs del Firewall

- **Objetivo:** Ver dónde se registran los eventos de firewall (si está configurado para logear).
- *Requisitos:* Firewall configurado (con reglas de LOG si usas iptables). Privilegios de superusuario (`sudo`).
- **Desarrollo Paso a Paso (Conceptual):**
    1. Abre una terminal.
    2. **Si usas `iptables` con reglas `LOG`:** Los mensajes de log van al log del kernel, típicamente accesible vía `dmesg` o journald. Ejecuta `dmesg | grep "IPT"` o `journalctl -k | grep "IPT"`.
    3. **Si usas `firewalld` o `ufw`:** Sus logs suelen ir al syslog del sistema o al journal. Usa `journalctl -f` y busca mensajes relacionados con `firewalld`, `ufw`, o mensajes de `kernel` con patrones de paquetes bloqueados si hay reglas de descarte.