📁 LPIC-2 / 🌐 Examen 207 - Servidor de Nombres de Dominio - Ejercicios

*Nota: Estos ejercicios implican explorar configuraciones de seguridad en BIND. Realízalos **SIEMPRE en una VM de prueba dedicada**. Modificar configuraciones de seguridad puede romper la funcionalidad si no se hace correctamente. Necesitarás privilegios de superusuario (`sudo`).*

Ejercicio 7.3.1: Verificando el Usuario Bajo el que Corre BIND y Permisos de Archivos de Zona

- **Objetivo:** Identificar el usuario dedicado de `named` y verificar si tiene permisos de lectura en los archivos de zona.
- **Requisitos:** BIND instalado. Privilegios de superusuario (`sudo`). Directorio de archivos de zona identificado (Ej. 7.2.1).
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.
    2. **Identifica el usuario de `named`:** Ejecuta `ps aux | grep named`. Busca la línea del proceso principal `named` y anota el nombre del usuario en la primera columna. Será `bind` o `named`.
    3. **Verifica la propiedad y permisos del directorio de archivos de zona:** Ejecuta `ls -ld <ruta_directorio_zona>` (ej: `ls -ld /var/lib/bind/` o `ls -ld /var/named/`).
    4. **Verifica la propiedad y permisos de un archivo de zona (ej: el de localhost):** Ejecuta `ls -l <ruta_archivo_zona_localhost>`.
    5. **Comprueba que el usuario de `named` tiene permisos de lectura:** Asegúrate de que el usuario identificado en el paso 2 tiene permisos de lectura (`r`) en el archivo de zona. A menudo, el grupo propietario del archivo o directorio será el grupo de `named`, y los permisos grupales incluirán lectura.

Ejercicio 7.3.2: Explorando la Configuración de Chroot (si aplica)

- **Objetivo:** Identificar si BIND está configurado para ejecutarse en un entorno chroot y explorar su estructura.
- **Requisitos:** BIND instalado. Privilegios de superusuario (`sudo`).
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.
    2. **Verifica el archivo de configuración de BIND (`named.conf`):** Busca la directiva `options { ... };` y dentro de ella la directiva `directory`. Si la ruta es `/` o un subdirectorio como `/var/named/chroot/` o `/var/lib/bind/chroot/`, puede indicar un chroot. Busca también la directiva `chroot` si está fuera del bloque `options`. A menudo, la configuración chroot se especifica en el archivo de unidad de systemd (`named.service` o `bind9.service`) o en scripts de inicio.
    3. **Verifica la unidad de Systemd (si usas systemd):** Ejecuta `sudo systemctl cat bind9.service` (Debian) o `sudo systemctl cat named.service`

(Red Hat). Busca la directiva `RootDirectory=` en la sección `[Service]`. Esto especifica el directorio chroot.

4. **Si se usa chroot, explora el directorio chroot (requiere sudo):** Ejecuta `sudo ls -l <ruta_directorio_chroot>`. Verás una estructura que simula el sistema de archivos raíz, conteniendo directorios como `etc`, `var`, `dev`.
5. **Explora los archivos de configuración y zona *dentro* del chroot:** Ejecuta `sudo less <ruta_directorio_chroot>/etc/named.conf` y `sudo less <ruta_directorio_chroot>/<ruta_archivos_zona>`. Estos son los archivos que BIND realmente lee cuando se ejecuta en chroot.

Ejercicio 7.3.3: Identificando Directivas de Control de Acceso en `named.conf`

- **Objetivo:** Localizar dónde se configuran las restricciones de consulta y transferencia.
- **Requisitos:** BIND instalado. Privilegios de superusuario (`sudo`) para leer `named.conf`.
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.
    2. **Visualiza el archivo de configuración principal:** Ejecuta `sudo less <ruta_a_named.conf>`.
    3. **Busca la directiva `allow-query`:** Puede estar en el bloque `options {}` (afecta a todas las zonas) o en bloques `zone {}` individuales. Una configuración segura en un servidor público a menudo permite consultas a `any` para zonas autoritativas, pero restringe la recursión.
    4. **Busca la directiva `allow-recursion`:** Normalmente en el bloque `options {}`. Si es un servidor público autoritativo, debería ser `allow-recursion { none; };` o `allow-recursion { <lista_ips_locales>; };`. Si es un servidor recursivo/forwarder interno, será `allow-recursion { <red_local>; };`.
    5. **Busca la directiva `allow-transfer`:** En los bloques `zone {}` para zonas maestras. Debería listar las IPs de los servidores secundarios autorizados. Si no está presente o dice `any`, cualquiera puede transferir la zona.

Ejercicio 7.3.4: (Conceptual) Limitando Consultas y Transferencias

- **Objetivo:** Entender cómo modificar `named.conf` para aplicar restricciones.
- *Requisitos:* Privilegios de superusuario (`sudo`). **VM de prueba.** IP de tu red local (ej: 192.168.1.0/24).
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.
    2. **Edita el archivo de opciones principal (requiere sudo):** `sudo vi <ruta_a_named.conf_options>`.
    3. **(Para un servidor recursivo interno):** Asegúrate de que `allow-recursion { <tu_red>; };` está configurado (ej: `allow-recursion`

`{ 192.168.1.0/24; };`). Esto evita que usuarios externos usen tu servidor para recursión.

4. **(Para un servidor autoritativo público):** Asegúrate de que `allow-recursion { none; };` o `{ localhost; };` está configurado.
5. **Guarda y sal.**
6. **Edita el archivo de configuración donde defines tu zona maestra (ej: `named.conf.local`):** `sudo vi <ruta_archivo>`.
7. **Añade o modifica la directiva `allow-transfer` en el bloque de tu zona maestra:**

```
zone "mytest.local" {
    type master;
    file "...";
    allow-query { any; }; // Puedes permitir consultas a todos si es
pública
    allow-transfer { <lista_ips_servidores_secundarios>; }; // IPs
de esclavos
    // Si no tienes esclavos, puedes poner none o dejarlo por
defecto si el default es restrictivo
    // allow-transfer { none; };
};
```

8. **Guarda y sal.**
9. **Verifica la sintaxis:** `sudo named-checkconf <ruta_a_named.conf>`.
10. **Recarga BIND:** `sudo systemctl reload ...`.
11. **Prueba:** Intenta consultar desde una IP no permitida (si es posible) o intenta una transferencia de zona (`dig axfr mytest.local @<IP_de_tu_VM>`) desde una IP no autorizada. Debería fallar.

Ejercicio 7.3.5: (Conceptual) Verificando DNSSEC con `dig +dnssec`

- **Objetivo:** Entender cómo ver si una zona está firmada con DNSSEC.
- **Requisitos:** Herramientas cliente instaladas. Conexión a internet.
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.
    2. **Consulta un dominio que sabes que usa DNSSEC (ej: .org, .gob):** Ejecuta `dig +dnssec dnssec-tools.org A`.
    3. **Observa la salida:** Deberías ver registros adicionales como `RRSIG` (firma del registro) y `DNSKEY` (claves públicas usadas para verificar la firma). El indicador `ad` (authenticated data) en la sección `HEADER` también indica que la respuesta fue validada por tu resolver.
    4. **(Concepto):** Esto no prueba que *tu* servidor BIND está configurado correctamente para validar DNSSEC (eso se configura en `options`), pero muestra cómo verificar si una zona está firmada y si tu camino de resolución (incluyendo tu servidor/resolver) está validando.

Ejercicio 7.3.6: Verificando Reglas de Firewall para DNS

- **Objetivo:** Asegurarse de que el firewall permite el tráfico DNS necesario.
- **Requisitos:** Privilegios de superusuario (`sudo`). Identificar la herramienta de firewall activa (Ej. 5.2.5).
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.
    2. **Si usas `firewalld` (Red Hat/CentOS/Fedora por defecto):** Ejecuta `sudo firewall-cmd --list-all` o `sudo firewall-cmd --zone=<zona> --list-services`. Asegúrate de que el servicio `dns` está permitido en la zona apropiada.
    3. **Si usas `ufw` (Debian/Ubuntu):** Ejecuta `sudo ufw status`. Busca reglas que permitan tráfico a/desde puerto 53 (UDP y TCP). Puedes añadir reglas si es necesario: `sudo ufw allow 53/udp` y `sudo ufw allow 53/tcp`.
    4. **Si usas `iptables` directamente:** Ejecuta `sudo iptables -L -v -n`. Busca reglas en las cadenas `INPUT` y `OUTPUT` que permitan tráfico a/desde el puerto 53.