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

207.3 Asegurar un servidor DNS

Teoría

Asegurar un servidor DNS es vital para la estabilidad y seguridad de tu red y de Internet en general. Un servidor DNS comprometido puede ser utilizado para redirigir tráfico a sitios maliciosos, ser parte de ataques DDoS (especialmente por amplificación si permite recursión abierta), o filtrar información interna a través de transferencias de zona no autorizadas.

Medidas de Seguridad Clave para BIND (`named`):

1. **Ejecución con Privilegios Mínimos (Usuario Dedicado):**
    - El demonio `named` no debe ejecutarse como `root`. Las distribuciones crean un usuario y grupo dedicados con los mínimos permisos necesarios para que `named` funcione.
    - **Nombre del Usuario/Grupo (Diferencias):**
        - **Rama Debian/Ubuntu:** Usuario y grupo `bind`.
        - **Rama Red Hat/CentOS/Fedora:** Usuario y grupo `named`.
    - **Permisos de Archivos de Zona:** Los archivos de zona deben ser propiedad de `root` (o del usuario que los crea/edita), pero deben ser legibles por el usuario bajo el que se ejecuta `named` (ej: `bind` o `named`). Los permisos de escritura deben estar restringidos al usuario administrador.
2. **Enjaulamiento (Chroot - Change Root):**
    - Ejecutar BIND en un entorno `chroot` (una "jaula"). Esto cambia el directorio raíz (`/`) del proceso `named` a un subdirectorio específico. Si BIND es comprometido, el atacante solo tendrá acceso a los archivos y directorios dentro de esa jaula, no a todo el sistema de archivos raíz real.
    - **Ubicación del Entorno Chroot (Diferencias):**
        - **Rama Debian/Ubuntu:** A menudo no está configurado por defecto, pero se puede instalar un paquete `bind9-hostutils` o similar que facilita la configuración chroot en `/var/lib/bind/chroot/` o rutas similares.
        - **Rama Red Hat/CentOS/Fedora:** Las versiones del paquete `bind` a menudo configuran el entorno chroot por defecto en `/var/named/chroot/`.
    - **Contenido del Entorno Chroot:** El directorio chroot debe contener una copia o enlaces simbólicos de los archivos y directorios necesarios para que `named` funcione dentro de la jaula (archivos de configuración, archivos de zona, `/dev/random`, `/dev/urandom`, librerías, archivos de resolución como `/etc/resolv.conf` y `/etc/nsswitch.conf`).
3. **Control de Acceso a Consultas (`allow-query`, `allow-recursion`):**
    - Controla quién puede consultar tu servidor DNS.

- `allow-query { <lista_ips_o_redes>; };`: En el bloque `options` o `zone`, permite que solo las IPs/redes listadas consulten el servidor (para consultas autoritativas o recursivas, dependiendo del contexto).
- `allow-recursion { <lista_ips_o_redes>; };`: En el bloque `options`, especifica qué clientes tienen permiso para realizar consultas recursivas. **¡CRUCIAL!** Un servidor DNS público que permite recursión a cualquiera es vulnerable a ataques de amplificación DDoS. Los servidores autoritativos públicos NUNCA deben permitir recursión a clientes externos. Los servidores internos para una red local sí permiten recursión para los clientes de esa red.

4. **Control de Acceso a Transferencias de Zona (`allow-transfer`):**
    - Controla qué servidores secundarios pueden obtener copias de tus zonas maestras. Exponer los datos de tu zona a atacantes puede darles información valiosa sobre tu infraestructura.
    - `allow-transfer { <lista_ips_servidores_secundarios>; };`: En el bloque `zone` para una zona maestra. Solo los servidores listados pueden solicitar transferencias AXFR/IXFR.
    - **¡NUNCA uses `allow-transfer { any; };` en un servidor autoritativo público!**
5. **Actualizaciones de Software:**
    - Mantén BIND y el sistema operativo actualizados. Las vulnerabilidades de seguridad en BIND son descubiertas periódicamente, y las actualizaciones incluyen parches críticos.
6. **Firewall:**
    - Configura el firewall del sistema (`firewalld`, `ufw`, `iptables`) para permitir solo el tráfico DNS necesario (puerto UDP 53 para consultas estándar, puerto TCP 53 para transferencias de zona y respuestas grandes) desde las fuentes autorizadas.
    - Si es un servidor autoritativo público, permite UDP/TCP 53 desde `any` para consultas autoritativas. Si es un servidor recursivo/forwarder interno, permite UDP/TCP 53 solo desde las IPs de tu red interna.
    - Si es un servidor primario para zonas con secundarios, permite TCP 53 desde las IPs de los servidores secundarios para transferencias de zona.
7. **DNSSEC (DNS Security Extensions):** (Conceptual para 207.3, detallado en 207.4 si estuviera listado)
    - Proporciona autenticación de origen de datos y protección de la integridad de los datos en DNS mediante firmas criptográficas.
    - Implementar DNSSEC requiere generar claves (ZSK, KSK), firmar las zonas y publicar registros DNSKEY y DS. LPIC-2 puede preguntar sobre el *concepto* y cómo verificar DNSSEC.
    - `dig +dnssec <nombre>`: Permite ver los registros DNSSEC (RRSIG, DNSKEY) si la zona está firmada y tu servidor o resolver soporta DNSSEC.

8. **Monitorización y Logs:**
    - Configura y revisa los logs de BIND para detectar intentos de acceso no autorizados, errores en la carga de zonas (posible indicio de intento de envenenamiento), alta actividad de consultas inusual (ataque DDoS), fallos en las transferencias de zona.
    - La configuración de logging se hace en `named.conf`. Los logs se pueden enviar a archivos específicos o al syslog del sistema (`journalctl`).
9. **Limitación de Tasa (Rate Limiting):** Configurar QPS (Queries Per Second) límites para diferentes tipos de consultas o fuentes para mitigar ataques DDoS.