



Published on hacktimes.com (<http://www.hacktimes.com>)

SECURIZACIÓN DE UN SERVIDOR DNS CON BIND

By vaxman

Creado 22 Dec 2005 - 11:57

Un sistema DNS es, básicamente, una base de datos distribuida y jerárquica que almacena información asociada a los nombres de dominio en redes como lo es Internet. Esta base de datos está mantenida por miles de servidores DNS y cada uno de ellos es responsable de una “zona” en Internet. Como base de datos, el DNS es capaz de asociar distintos tipos de información a cada nombre, pero sus usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

Como es mucho más sencillo recordar el nombre o la URL de una página web que toda su dirección IP, la asignación de nombres de dominio a direcciones IP, que es como funcionan realmente los sistemas en Internet, es la función más conocida de un sistema DNS, así, si por ejemplo, si la dirección IP del sitio FTP de hacktimes.com fuera 169.100.100.4, todo el mundo llega a este equipo especificando ftp.hacktimes.com y no teniendo que especificar la dirección IP.

Además de ser más fácil de recordar, el nombre es más fiable ya que la dirección numérica puede cambiar por diversos motivos sin que por ello se tenga que cambiar el nombre.

Se dice también que un DNS es una base de datos jerárquica porque los nombres de dominio no son más que nodos que descienden de la raíz de la base de datos representada por el nodo "." al estilo de como funcionan los sistemas de ficheros en Unix. Los Servidores DNS (Servidores de Nombres de Dominio) son los nodos en los que reside la aplicación que traduce los nombres de dominio a direcciones IP y viceversa.

Debido a todo esto, en un sistema DNS se almacena diversa información acerca de los sistemas de una entidad: todos los nombres de dominio asociados al dominio principal, el listado de máquinas de toda una red con sus nombres y direcciones IP, etc. lo que permite, entre otras cosas, hacer un mapeo de los diferentes sistemas de una red en concreto a la hora de buscar posibles objetivos y encontrar vulnerabilidades y/o debilidades en el sistema.

Entre los ataques característicos a un sistema DNS, además de las vulnerabilidades que puedan existir en el software utilizado, destacan la resolución de nombres, las

transferencias de zona, el DNS Spoofing y, últimamente, el pharming. Este artículo que se centra en el software BIND (BERKELEY INTERNET NAME DOMAIN) que es el más conocido y usado en Internet como servidor de DNSs, explicará como securizarlo para evitar esos errores de configuración que puedan comprometer todo el sistema, facilitar información a un posible atacante o, minimizar el riesgo en caso de una intrusión.

SECURIZACIÓN

Una vez que la última versión del software BIND [1], la última disponible es la v.9.3.1, está instalada o hemos actualizado el sistema a esta versión, y el servidor está funcionando correctamente, se han de seguir los siguientes pasos a modo de lista de comprobación, para proceder a aumentar el nivel de seguridad de la plataforma:

- **MANTENERSE AL DÍA** acerca de las vulnerabilidades existentes para BIND mediante las páginas típicas de SecurityFocus [2], SecuriTeam [3], etc. para así saber si existe una versión del software más actual que la que tenemos instalada o se ha sacado alguna versión nueva de BIND que corrige diversos fallos y vulnerabilidades encontradas en versiones anteriores o incluso incluye nuevas funcionalidades.
- **INSTALAR BIND DETRÁS DE UN CORTAFUEGOS:** muchos problemas de seguridad no dependen directamente del software BIND así que, además de securizar el servidor y el sistema operativo bajo el que se instala BIND, es preciso instalar un sistema de firewall antes que el DNS para así reducir más los posibles ataques y limitar los accesos al servidor.
- Si es posible, **DISPONER DE UN SERVIDOR DE RESPALDO:** por temas de redundancia es recomendable disponer de servicios duplicados tanto a nivel de servidor como de conectividad, disponiendo incluso de ISPs diferentes para así conseguir una alta disponibilidad en el servicio. El servicio DNS como se está viendo, es demasiado crítico como para que un error de hardware por ejemplo deje a una empresa sin servicio.
- **UTILIZAR UN SERVIDOR DEDICADO:** uno de los errores más comunes es el de utilizar el mismo sistema para el servidor de nombres interno y externo o compartir el sistema DNS con otro servicio, algún servidor web u otro sistema. Es recomendable emplear una máquina independiente y dedicada para el servicio DNS ya que es demasiado crítico y cualquier configuración incorrecta de servicios superfluos puede comprometer toda la infraestructura de la entidad en Internet dejándola sin servicio. El servidor dedicado debe de estar previamente securizado a nivel de sistema operativo.
- **RESTRINGIR LAS CONSULTAS DNS:** lo lógico es que el servidor DNS de la entidad no acepte consultas (ni recursivas ni peticiones corrientes) de

sistemas de fuera de la red confiable, mediante el uso de ACLs se limita en el fichero de configuración del BIND (named.conf):

```
acl mired { 10.104.48/24; } // este sería la red de la entidad
allow-query { mired; }; // sólo se admiten consultas de la red de la
entidad
```

- **EVITAR EL USO DE LA CACHÉ DNS:** BIND, sobretodo en sus versiones antiguas, responde por defecto a las peticiones que se le hacen con la información de su zona y su memoria caché que ha ido completando a partir de las consultas con otros servidores. Existen situaciones en las que es conveniente evitar esa caché ya que no se puede garantizar su corrección o simplemente porque ésta es innecesaria, esto ocurre, por ejemplo, si el servidor DNS es un servidor secundario o esclavo de una zona que no es totalmente segura, o que sea el responsable de una zona determinada, etc.
- **NO EJECUTAR BIND COMO ROOT:** Ejecutar el servicio de DNS (al igual que el resto de servicios) con un usuario sin apenas privilegios, nunca como root para minimizar el riesgo en el caso de que el servicio haya sido comprometido. Esta es la tendencia en los recientes sistemas Linux que ya permiten ejecutar BIND con un usuario diferente al de root (NAMED), sin privilegios, que pertenece al grupo NAMED y que además no tiene acceso a ninguna shell (/bin/false) ya que no la necesita:
 - Introducir en el fichero /etc/passwd:
dns:*:uid:gid:Cuenta del servicio
BIND:/home/dns:/bin/false
 - Y en el fichero /etc/group:
dns:x:gid
 - Arrancar el servicio con el usuario creado sin privilegios:
daemon named -u dns -g dns
- **RESTRINGIR LAS TRANSFERENCIAS DE ZONA:** para configurar los controles de acceso (ACLs) es recomendable restringir las transferencias de zona y así minimizar la cantidad de información disponible para un usuario malintencionado. Estudiar la consideración de no permitir consultas recursivas o ser más restrictivo. De esta forma, también se evita que se pueda suplantar a un servidor DNS esclavo y extraer toda la información de la zona de la que es servidor.
- **RESTRINGIR LAS ACTUALIZACIONES DINÁMICAS:** De forma similar a lo que ocurre con las transferencias de zona, es aconsejable restringir qué sistemas pueden realizar actualizaciones dinámicas. Su configuración se realiza también con listas de control de acceso (ACLs) mediante la opción allow-update.

- **EMPLEAR TSIG (Transaction SIGnatures):** El uso de ACLs para controlar las actualizaciones dinámicas, las transferencias de zona y las consultas recursivas no es demasiado seguro ya que con un simple paquete UDP en el que se ha falsificado la dirección origen, un atacante se podría hacer pasar por uno de los sistemas permitidos en las listas de control de acceso.

Por todo ello, se introduce la técnica criptográfica de autenticación, HMAC-MD5, para garantizar la transferencia de la información y la integridad de todas las comunicaciones DNS. TSIG es útil para la comunicación entre servidores o entre un servidor y un sistema actualizador pero si se han de administrar múltiples servidores se corre el riesgo de que si la clave compartida de alguno de ellos es comprometida, se compromete todo el sistema así que para ello se utiliza mejor las firmas DNSSEC.

- **UTILIZAR DNSSEC:** Se recomienda firmar digitalmente las zonas del servicio DNS para así garantizar su autenticidad e integridad y evitar ciertos ataques de DNS Spoofing. Mediante las extensiones de seguridad para el protocolo DNS, DNSSEC, se consigue firmar digitalmente todos los ficheros de zona configurados mediante el uso de sistemas de criptografía de llave pública. La última versión disponible en el momento de este artículo, la 9.3.1 ya incluye soporte nativo para las extensiones DNSSEC.

- **CONFIGURAR BIND** para que no informe acerca de la versión del software instalado: Ofuscar en la configuración del fichero `named.conf` la posibilidad de realizar consultas tipo “`bind.version`” para extraer la versión del software instalado y buscar, posteriormente, vulnerabilidades conocidas. Introducir en el fichero `named.conf` la siguiente línea en el apartado de options:
`version "LO_QUE_SE QUIERA_INDICAR";`

- **AISLAR EL SERVICIO DNS:** Es recomendable ejecutar el servicio DNS en un entorno aislado, en lo denominado jaula “chroot” para dificultar que si el servicio DNS ha sido comprometido, esto pueda afectar al resto de servicios disponibles o al mismo sistema operativo del servidor.

Para construir un entorno aislado chroot es necesario:

- Crear los siguientes directorios:

```
mkdir -p /chroot/named
mkdir /chroot/named/dev
mkdir /chroot/named/lib
mkdir /chroot/named/etc
mkdir -p /chroot/named/usr/sbin
mkdir -p /chroot/named/var/run
mkdir /chroot/named/var/named
```

```

Copiar los siguientes ficheros de configuración:
cp /etc/named.conf /chroot/named/etc
cp -a /var/named /chroot/named/var/named
mknod /chroot/named/bin/false c 1 3
chmod 666 /chroot/named/bin/false
cp /usr/sbin/named /chroot/named/usr/sbin
cp /usr/sbin/named-xfer /chroot/named/usr/sbin

```

- Cambiar el propietario de los directorios de la jaula chroot para que sea el mismo que ejecute el servicio named:

```
chown -R dns:dns /chroot/named/var/named
```

- **MODIFICAR LOS TIEMPOS DE REFRESCO:** para evitar ciertos ataques de Denegación de Servicio (DoS) es recomendable mantener una configuración segura de los tiempos de refresco del servicio DNS Primario y del registro de inicio de autoridad de los archivos de zona (SOA).

Parámetro DNS	Valor Recomendable	Descripción
SOA Refresh	Entre 3600 - 7200	Especifica el intervalo de actualización de una zona
SOA Retry	Entre 1200 - 7200	Especifica el intervalo de reintento de una zona
SOA Expire	Entre 2 y 4 semanas	Especifica el intervalo de caducidad de una zona
SOA Minimum TTL	Entre 3600 - 86400	Especifica el valor de Período de vida (TTL) mínimo. Indica el espacio de tiempo utilizado por otros servidores DNS para determinar cuánto tarda la información en caché de un registro de una zona en caducar y descartarlo.
SOA Serial Number		El formato recomendable para identificar un servicio DNS es YYYYMMDDnn, donde 'nn' es el número de revisión. Este número ha de irse incrementando cada vez que se realice alguna modificación en el servicio DNS.

- **MONITORIZAR Y REGISTRAR** la actividad del servicio DNS: Realizando una monitorización del servicio DNS es posible detectar numerosos problemas que puedan suponer una degradación del servicio, por otro lado, si se realiza un registro de toda la actividad del servicio se pueden detectar cambios no autorizados que puedan comprometer la integridad del servicio. Añadir la siguiente línea en la configuración del syslog:

```
daemon syslog -m 0 -a /chroot/named/dev/log
```

Source URL:

<http://www.hacktimes.com/?q=node/27>

Links:

[1] <http://www.isc.org/products/BIND/>

[2] <http://www.securityfocus-com>

[3] <http://www.securiteam.com>