# Vulnerabilidad en DNS

Por Téc. Vladimir Molina Ruiz, Adm.or de Red, Ing. Marisley Guevara Fernández, Esp. B Ciencias Informáticas, Lic. Antonio Tarajano Roselló, Prof. Instructor, Cátedra de Gestión de Información en Salud, Universidad de Ciencias Médicas "Carlos J. Finlay", e Ing. Yudelkis Abad Fuentes, Jefa de Asignatura Sistema Operativo y Seguridad Informática en la Facultad 6 de Bioinformática, Universidad de las Ciencias Informáticas (UCI).
vladimi@finlay.cmw.sld.cu, mguevara@finlay.cmw.sld.cu, tarajano@finlay.cmw.sld.cu, yabad@uci.cu,

## 1 Introducción

El DNS —del inglés, *Domain Name System* / Sistema de Nombres de Dominio— es una base de datos distribuida y jerárquica que almacena la información necesaria para los nombres de dominio o gestiona nombres de equipos y servicios en redes locales [1],[2]. Sus usos principales son la asignación de nombres de dominio a direcciones IP; la traducción de una dirección IP en una o varias direcciones canónicas —conocida como resolución inversa—; y la localización de los servidores de correo electrónico correspondientes para cada dominio. El DNS nació a partir de la necesidad de facilitar a las personas el acceso hacia los servidores disponibles en Internet, a través de un nombre, recurso que resulta mucho más fácil de recordar que una dirección IP.

Dada la importancia que adquiere en la actualidad el tema de la seguridad de los servidores DNS, el presente trabajo se propone identificar aspectos relevantes que se deben tener en cuenta para la correcta configuración de los mismos. En este sentido, se identifican las características de los DNS desde el punto de vista de la seguridad informática y se exponen medidas que permiten solucionar problemas generados por su inadecuada configuración. Luego, se establece una propuesta de configuración del named.conf, aplicada en estos momentos en la red Infomed, en Camagüey.

## 2 Desarrollo

El DNS establece la ruta a seguir por cualquier sistema o datos que se intercambian por Internet. Esto significa que no importa cuán seguro sea un servidor Web, de correo, o cualquier otro, si el DNS se encuentra expuesto a riesgos. Entonces, sus aplicaciones manifestarán un elevado índice de vulnerabilidad a posibles ataques desde Internet.

El BIND —*Berkeley Internet Name Domain* / Nombre de Dominio de Internet de Berkeley— es el servidor DNS más utilizado en los sistemas operativos Linux en cualquiera de sus tres versiones:

- V4, que ha sido abandonada por la mayoría de los vendedores.
- V8, que es valorada por su alto nivel de complejidad, aunque ya se considera caduca.
- V9, versión libre y comercialmente patrocinada. Posee rasgos novedosos que le otorgan un mayor nivel de seguridad.

Debido a estas características, la presente investigación se centra en la utilización de los servidores Bind9.

### 2.1 DNS Bind9

El BIND está compuesto por varios archivos que permiten agregar y modificar algunos parámetros de funcionamiento del servidor DNS. Dentro de ellos se encuentran:

- **named.conf**: archivo principal donde se especifican las zonas y la ubicación de sus archivos.
- **named.conf.options**: establece la mayoría de las opciones del servidor. Permite definir el comportamiento del mismo, por ejemplo, las redes, los derechos de transferencia, entre otros aspectos.
- **db.0 db.127 db.local db.255**: archivos de zonas predefinidas para la red local e Internet.
- **db.root**: archivo que contiene la información de todos los *DNS* de nivel superior (*Root Servers*).

Dentro de las instrucciones que determinan el accionar del named.conf, se encuentran las Zonas. Estas no son más que archivos en donde se establece la información de un dominio. Para crear una nueva zona, primero ha de especificarse la ruta del archivo de zona.

Esto se hace en el interior del archivo, donde ya existen zonas predeterminadas. La ruta para este archivo sería la siguiente: /etc/bind/named.conf.

### 2.2 DNS no seguro

La utilización de un DNS no seguro, o comprometido, puede causar muchos daños. En este sentido, los principales son:

1-Obtención de información. En este caso, el riesgo estará determinado por la no definición de quienes tienen permiso para realizar transferencias de zonas. El atacante puede obtener, entre otros datos, la lista completa de computadoras (*hosts*) y encaminadores (*routers*), con sus direcciones IP, nombres y, posiblemente, comentarios que indiquen su situación.

2-Denegación de Servicio —*Denial of Service* (DoS)—: si todos los servidores de DNS caen:

- El sitio Web (*Website*) ya no es visible —los otros sitios no pueden resolver su dirección IP —.
- Los correos electrónicos no pueden ser enviados —algunos sitios en Internet con los cuales intercambia información a menudo habrán guardado en su caché los registros de DNS—.
- Un atacante podría iniciar un falso servidor de DNS que finge ser el suyo y envía información de DNS falsa a Internet acerca de su dominio.

3-Pérdida de integridad: un atacante puede cambiar los datos del DNS o facilitar —mediante envenenamiento (*spoofing*) — a otros sitios información falsa, esto se conoce como envenenamiento de DNS. Ello incluye:

- Falsificar el sitio Web y capturar las entradas de los usuarios que iban destinadas al mismo. Se favorece, así, el **robo** de nombres de usuario, contraseñas y números de tarjetas de crédito.
- Redireccionar el correo a un servidor repetidor (*relay*), que podría copiar, cambiar o borrar el correo antes de pasarlo al sitio.
- Comprometer el cortafuego (*firewall*) o cualquier *host* accesible desde Internet, especialmente si un filtro de paquetes débil es quien protege los Servidores de Internet y la Intranet, hecho que potencializa la utilización de nombres de *host* de DNS —DNS *hostnames*— para autenticarse o para relaciones de confianza [3].

### 2.3 Metodología de diseño

Para el diseño de la aplicación, se presenta un mapa conceptual del algoritmo de trabajo establecido (Figura 1). Se enfatiza —cuadro en rojo—, la parte descrita en la presente investigación. La misma sentó las bases para la identificación de los parámetros de configuración de un servidor de DNS. Por otra parte, también se delinearon medidas de prevención para evitar riesgos en estos servidores.

El DNS es un sistema cliente/servidor. Los servidores (de nombres) cargan los datos de sus ficheros de DNS en memoria y los usan para responder las consultas tanto de los usuarios de la red interna como de los usuarios y otros servidores en la red Internet.

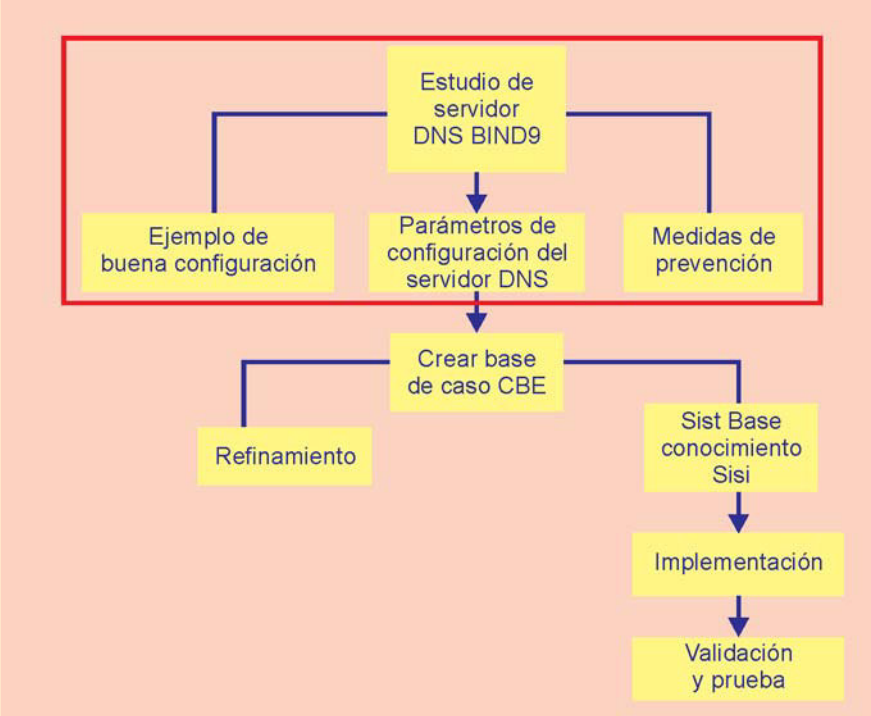


Figura 1 Fases del trabajo. (Fuente: elaboración propia).

Como se ha mencionado con anterioridad, en un sistema DNS se almacena información acerca de los sistemas de una entidad: todos los nombres de dominio asociados al dominio principal, el listado de máquinas de la red con sus nombres y direcciones IP, entre otros aspectos. Esto permite realizar un mapeo de los diferentes sistemas de una red en concreto a la hora de buscar posibles objetivos y encontrar vulnerabilidades o debilidades en el sistema [4]. A continuación se muestran una serie de **parámetros** que debe cumplir un DNS para ser confiable.

- Ocultar la versión "DN*S* server".
- Creación de una nueva llave TSIG —*Transaction SIGnatures* / Transacciones Firmadas— con la sintaxis dnssec - keygen - a HMAC - MD5 - b 512 - n HOST/ —Algoritmo HMAC"MD5, de 512 bits y tipo HOST—.
- Transferencias seguras con *Key* —Llaves Seguras— a Servidores Primarios (*Masters*) y Servidores Secundarios (*Slaves*).

- Delimitación de la recursión a redes o red, en específico, con sintaxis o sentencia allow-recursion{192.168.0.0/24;}.
- Seguridad en la transferencia de zonas de los DNS primarios, con la sentencia allow-transfer {192.168.0.1;}.
- Delimitación de las consultas a *host*, propiamente, con la sentencia allow-query {host;}.
- Utilizar DNS Security con la sentencia en archivo de configuración DNSSEC —*DNS Security Extensions* / Extensiones de Seguridad DNS— que permite a los servidores DNS firmar sus respuestas.
- Actualización Dinámicas de las Llaves y las ACL —*Access Control List* / Lista de Control de Acceso— allow-update {key updater; updaters;};
- Servidor DNS (Bind), actualizado en su última versión.
- Configurar DNS con las Sentencias *view* o vistas en español (Interna) y (Externa).
- Configurar la Personalización de los *Logs* del Servicio DNS.

### 2.4 Medidas preventivas

Los riesgos del Bind pueden ser reducidos considerablemente con algunas medidas de prevención:

1. Aislamiento de los recursos: debe utilizarse un servidor dedicado y asegurado para el DNS de Internet, no ha de compartirse con otros servicios y, especialmente, no se debe permitir el acceso remoto del usuario. Minimizar los servicios y usuarios significa reducir la cantidad de software en ejecución y, por lo tanto, la probabilidad de exponerse a ataques de red. La separación previene contra la posibilidad de que otros servicios o usuarios localicen debilidades en el sistema y las usen para atacar a Bind.
2. Redundancia: debe instalarse un secundario (*slave*) en una conexión a Internet diferente —rama alejada de la empresa, u otro ISP —*Internet Service Provider* / Proveedor de Servicios de Internet—.
3. Utilización de la última versión del DNS Bind9.
4. Control del acceso: debe restringirse la transferencia de zonas para minimizar la cantidad de información que está disponible en su red para los atacantes. Debe considerarse el uso de transacciones firmadas y, además, la restricción o prohibición de las consultas recursivas.
5. Ejecución de Bind con los mínimos privilegios: como usuario no *root* —privilegios de administración—, con una máscara (*umask)* muy restrictiva, por ejemplo, 177.
6. Mayor aislación de recursos: debe ejecutarse Bind en un entorno *jail* (jaula) de modo que sea mucho más difícil que un Servidor DNS comprometido dañe el sistema operativo o afecte otros servicios.
7. Configuración del DNS (Bind) para que no informe de su versión. Esta medida representa seguridad por ocultación, ello protege contra atacantes con *scripts* (códigos) que rastrean la red en busca de objetivos obvios.
8. Detección: deben monitorizarse los *logs* en la búsqueda de alguna actividad inusual y cambios no autorizados en el sistema mediante un analizador de integridad.
9. Ha de mantenerse continuamente actualizado de las novedades y asegurar la notificación de la salida de nuevos problemas de DNS Bind en un tiempo razonable.

Esta serie de medidas permite configurar el DNS de una manera confiable. A continuación se establece un ejemplo de configuración del named.conf

### 2.5 Configuración del named.conf en la red Infomed de Camagüey

```
options {
        directory "/var/named/";
        dump-file  "/var/named/data/cache_dump.db";
        dnssec
        statistics-file  "/var/named/data/named_stats.txt";
        # hide our "real" version number
        version       "[secured]";
        default-server  localhost;
        default-key    rndc_key;
        allow-recursion  {
                127.0.0.1;
                192.168.1.0/24;
        };
        forwarders {
                200.33.146.209;
                200.33.146.217;
        };
        forward first;
controls {
inet 127.0.0.1 allow {
127.0.0.1;
}
keys {
"prueba.ejemplo.com.";
};
};
server 200.19.18.1 {
keys {
"  prueba.ejemplo.com.";
};
};
```

Por su parte, en el /etc/bind/named.conf del servidor secundario se añadirá la siguiente configuración:

```
controls {
inet 127.0.0.1 allow {
127.0.0.1;
}
keys {
“  prueba.ejemplo.com.”;
};
};
server 200.19.18.2 {
keys {
“  prueba.ejemplo.com.”;
};
};
acl slaves {
    200.18.189.2;
};
acl interna {
    127.0.0.1;
    192.168.0.0/24;
};
acl externa {
    200.18.19.0/24;
};
view “interna” {
match-clients { ppp; !any; };
allow-recursion { int; };
zone “.” {
   type hint;
   file “/etc/bind/db.root”;
   };
zone “localhost” {
   type master;
   file “/etc/bind/db.local”;
   };
zone “127.in-addr.arpa” {
   type master;
   file “/etc/bind/db.127”;
   }
zone “prueba.ejemplo.com” IN {
   type master;
    file “dominio.interno.db”;
    allow-transfer { none; };
    allow-update { none; };
   update-policy { update_policy_rule; [...] };
   notify yes;
      };
zone “0/1.0.168.192.in-addr.arpa” {
       type master;
       file “dominio.interno_rev.192.168.0.1”;
       };
};
view “externa” {
     match-clients { fr; !any; };
      allow-recursion { no; };
      allow-transfer {slave; };
      allow-update {key  updater; slave;};
zone “.” {
   type hint;
```

```
   file “/etc/bind/db.root”;
   };
zone “localhost” {
   type master;
   file “/etc/bind/db.local”;
   };
zone “127.in-addr.arpa” {
   type master;
   file “/etc/bind/db.127”;
   };
zone “ prueba.ejemplo.com “ IN {
   type master;
   file “dominio.externo.db”;
   allow-transfer { none; };
   allow-update { none; };
   notify yes;
      };
zone “24/0.19.18.200.in-addr.arpa” {
      type master;
      file “ dominio.externo_rev.200.18.19.1”;
      };
};
logging {
category “default” { “debug”; };
category “general” { “debug”; };
category “database” { “debug”; };
category “security” { “debug”; };
category “config” { “debug”; };
category “resolver” { “debug”; };
category “xfer-in” { “debug”; };
category “xfer-out” { “debug”; };
category “notify” { “debug”; };
category “client” { “debug”; };
category “unmatched” { “debug”; };
category “network” { “debug”; };
category “update” { “debug”; };
category “queries” { “debug”; };
category “dispatch” { “debug”; };
category “dnssec” { “debug”; };
category “lame-servers” { “debug”; };
channel “debug” {
file “/var/log/bind.log” versions 2 size 50m;
print-time yes;
print-category yes; };
};
```

## 3 Conclusiones

En la investigación presentada, se realizó un estudio del servidor DNS Bind9, en el que se recogen los aspectos básicos para su buen uso y configuración, dados por:

- 11 parámetros fundamentales que debe tener dicho servidor para presentar buena seguridad.
- Se mencionan varios archivos que componen el Bind. Estos pueden agregarse y modificarse con lo que se cambiaría el funcionamiento del servidor DNS. Ellos son: named.conf, named.conf.options, archivos de zonas predefinidas para la red local e Internet: db.0 db.127 db.local db.255, así como los archivos que contienen la información de todos los DNS de nivel superior: db.root.

◆ Se explica cómo los riesgos de un DNS no seguro o comprometido pueden causar daños a la red, tal es el caso de la información —computadoras y encaminadores con sus direcciones IP— a los que puede acceder un atacante si se permite transferencias de zonas. Pueden existir, además, problemas de denegación de servicios y pérdida de integridad de la información.

◆ A partir de los riesgos que puede presentar un DNS no seguro se proponen 9 medidas preventivas que pueden contrarrestar los ataques de intrusos a la red.

Como resultado de la investigación, se establece una propuesta de configuración de DNS que en estos momentos se encuentra implementada en la red de salud en Camagüey.

## 4 Referencias bibliográficas


[1] "Instalación de un DNS con bind". (diciembre/2008). *Liberalia Tempus: Servicios Informáticos*. http://www.liberaliatempus.com/dns-bind.html. (acceso enero 10, 2009).

[2] Barrios Dueñas, Joel. "¿Cómo configurar un servidor de nombres de dominio (DNS) en Red Hat O Cent OS 5"? (mayo/2008). http://www.linuxparatodos.net/portal/staticpages/index.php?page=como-dns. (acceso noviembre 23, 2008).

[3] Boran, Seán. "Running the BIND9 DNS Server securely". (mayo/2008). www.boran.com/security/sp/bind9_20010430.html. (acceso enero 15, 2009).

[4] "Securización de un servidor DNS con BIND". (Diciembre/2005). http://www.hacktimes.com/files/Securizacion-DNS-BIND-HackTimes.com.V.1.0.pdf. (acceso noviembre 23, 2008).