Las vulnerabilidades de seguridad de DNS

Jhon Francined Herrera C.

Recibido el 17 de febrero de 2009. Aprobado el 27 de abril de 2009

Resumen
El Sistema de Nombres de Dominio (DNS) es una base de datos distribuida que permite la traducción de direcciones IP a nombres particulares para la localización de recursos registrados a través de la red. Pero al igual que cualquier sistema distribuido, afronta diferentes problemáticas que afectan la integridad y consistencia de la información que maneja, problemáticas que se contextualizan en vulnerabilidades de seguridad tanto en el flujo de datos como en la infraestructura DNS.

En este artículo se presenta una revisión inicial de los aspectos de seguridad en DNS, pasando posteriormente a concretar las principales vulnerabilidades de seguridad a las que se enfrenta el sistema DNS, originadas por una variedad de circunstancias que serán tenidas en cuenta en la sección de técnicas y recomendaciones.

Palabras clave
Vulnerabilidad de Seguridad, DNS, Ataques DNS, Sistema Distribuido, Configuración DNS

Abstract
The Domain Name System (DNS) is a distributed database that allows the translation of private IP addresses to names for the location of resources recorded by the network. But like any distributed system, faces different problems affecting the integrity and consistency of the information handled, this problem are contextualized in security vulnerabilities in both the flow of data in the DNS infrastructure.

This article presents an initial review of safety aspects in DNS, then going to realize the major security vulnerabilities faced by the DNS system, caused by a variety of circumstances to be taken into account in the technical section and recommendations.

Key words
Security Vulnerability, DNS, DNS attacks, Distributed Systems, DNS Configuration

I. Introducción

En un mundo globalizado como el actual, la necesidad de comunicarse y compartir información intra e inter organizaciones ha adquirido cada vez mayor relevancia e importancia en el interior de cada organización.

Como una forma de suplir estos requerimientos, el mundo de la tecnología e infraestructura de comunicaciones ha evolucionado a grandes pasos, para suplir las exigencias del mundo moderno.

Para afrontar este reto e introducirse en la dinámica de crecimiento, ampliación e innovación de servicios, cobertura de nuevos mercados, entre otros aspectos, cada organización ha implementado diferentes tipos de soluciones y estrategias para el control, almacenamiento y gestión de su información, que con el tiempo ha actualizado, modificado o cambiado totalmente acorde a sus posibilidades y limitaciones organizacionales, en otras palabras, ha implantado tecnologías, equipos, herramientas, etc., en la medida en que sus capacidades económicas, tecnológicas y de infraestructura lo ha permitido.

Ahora bien, las organizaciones no se quedan estancadas en un lugar o mercado, ofreciendo un mismo tipo de servicio, por el contrario, se diversifican, amplían su alcance geográfico, se fusionan, etc. Derivada de la evolución y el crecimiento organizacional se genera una nueva necesidad: comunicar sistemas heterogéneos, ubicados en diferentes lugares geográficos, necesidad que se afronta con los sistemas distribuidos, que tratan de dar solución a estos requerimientos.

Un ejemplo de los retos que afronta un sistema distribuido es el gran mundo de Internet, donde cada recurso o máquina debe ser ubicable y accesible desde cualquier lugar geográfico, plataforma, etc., requiriendo para ello de un identificador único que la haga diferenciable entre las demás, y para ello se apoya en el uso de direcciones IP, tal como 200.21.30.10. Estas direcciones se componen de un conjunto de números que en algunas ocasiones se tornan complejos para las personas comunes que requieren acceder a los recursos, por lo cual, cada recurso tiene asociado también un nombre, tal como puede ser, a efectos de ejemplo www.presidencia.gov.

Desde la perspectiva de un usuario, cada nodo o recurso sobre esta red se identifica por un nombre único junto con un nombre de dominio como www.nist.gov. Sin embargo, desde la perspectiva de los equipos de redes de comunicaciones que enrutan las comunicaciones a través de Internet, el identificador único de un recurso es una dirección de protocolo de Internet (IP). Para acceder a los recursos de Internet, los nombres de dominio son más amigables que las direcciones IP, por lo que los usuarios necesitan un sistema que traduzca nombres de dominio a direcciones IP y viceversa. Esta traducción es la tarea principal del sistema de nombres de dominio – DNS (Chandramouli, 2006). La infraestructura de un DNS está diseñada para comunicar entidades distribuidas por todo el mundo, en otras palabras, ser un directorio global jerárquico distribuido que traduce nombres de máquina en direcciones IP numéricas.

Como todo sistema distribuido, DNS no es ajeno de afrontar diferentes problemáticas de escalabilidad, transparencia, heterogeneidad y de seguridad, más aún cuando los datos manejados por DNS están destinados a ser de dominio público, y su infraestructura inicial no contemplaba la definición de una alta seguridad.

Enfocándose en aspectos de seguridad y teniendo en cuenta que el principal objetivo de DNS es garantizar la autenticidad de la información del nombre de dominio y mantener la integridad de la información del mismo, resaltando que DNS es susceptible a los mismos tipos de vulnerabilidades (plataforma, software y de nivel de red) como cualquier otro sistema de computación distribuida, el presente artículo se enfoca en analizar, desde la óptica de sistemas distribuidos, las principales vulnerabilidades en seguridad presentadas en DNS.

Para ello, el documento se divide en varias secciones que permiten involucrar de manera progresiva los aspectos relacionados con los sistemas DNS, diferenciar las principales vulnerabilidades presentadas, partiendo desde una revisión muy rápida de los ataques de hacking, virus, etc. (los cuales no se profundizan, debido a que correspondería a un artículo sobre seguridad), hasta las vulnerabilidades producidas por errores en la configuración, y culminar con algunas de las principales técnicas generadas para contrarrestar estas vulnerabilidades; y finalmente, se presentan las conclusiones del trabajo y la revisión realizada.

II. Background

DNS, que en sus orígenes surgió como una posible solución a la problemática de extender el direccionamiento del correo electrónico, ha pasado a ser un servicio crítico adquiriendo gran importancia dentro del ámbito de Internet como medio de acceder rápidamente a los recursos que estén disponibles a través de la red. Pero al igual que cualquier sistema de computación distribuida, DNS es susceptible de múltiples vulnerabilidades, tales como problemas en la plataforma, software y capas de red, entre otras; de la misma forma como aplican al DNS los objetivos de seguridad tales como confidencialidad, integridad y disponibilidad de la información (Radack, 2006).

DNS se constituye como una base de datos distribuida, muy escalable, que se gestiona de forma des-

centralizada utilizando delegación, implementada como una jerarquía de servidores DNS que almacenan información sobre recursos registrados en cada uno de ellos (Díaz, 2003).

Para llevar a cabo su tarea, la organización jerárquica de DNS se dispone en zonas y se distribuye entre los servidores, donde cada zona está disponible en 2 ó más servidores manejando, como lo describe Bellido (2007), un flujo de datos entre:

Servidor primario que almacena la información de su zona en una base de datos local. Es el responsable de mantener la información actualizada y cualquier cambio es directamente cargado en este servidor.

Servidores secundarios. Son aquellos que obtienen los datos de su zona desde otro servidor que tenga autoridad para esa zona (un primario o algún otro secundario). El proceso de copia de la información se denomina transferencia de zona.

Servidores maestros (master servers). Son los que transfieren las zonas a los servidores secundarios. Cuando un servidor secundario arranca busca un servidor maestro y realiza la transferencia de zona. Un servidor maestro para una zona puede ser a la vez un servidor primario o secundario de esa zona. Estos servidores extraen la información desde el servidor primario de la zona. Así se evita que los servidores secundarios sobrecarguen al servidor primario con transferencias de zonas.

Servidores locales (caching-only servers). Los servidores locales no tienen autoridad sobre ninguna zona; se limitan a contactar con otros servidores para resolver las peticiones de los clientes DNS. Estos servidores mantienen una memoria caché con las últimas consultas respondidas. Cada vez que un cliente DNS le formula una pregunta, primero consulta en su memoria caché. Si encuentra la dirección IP solicitada, se la devuelve al cliente; si no, consulta a otros servidores, apunta la respuesta en su memoria caché y le comunica la respuesta al cliente.

El anterior flujo de datos representa un alto porcentaje de la vulnerabilidad en seguridad, por lo que actualmente existe una fuerte demanda de aseguramiento en comunicaciones entre sistemas DNS, los cuales no prevén, por ejemplo, ataques de modificación o inyección de mensajes DNS, negación de servicios, etc. (Ateniese et al., 2001; Kaminsky, 2003; Vasileios et al, 2004).

Pero no solamente por su naturaleza distribuida y la función crítica que desempeña, DNS se ve también afectado por los errores a la hora de crear una arquitectura DNS, a tenor de la amplia variedad de ataques sufridos últimamente en Internet. Un reciente estudio realizado por The Measurement Factory[1], asegura que más de la mitad de los servidores de nombres de Internet están mal configurados, dejando las redes abiertas a ataques y causando graves daños tanto a empresas como a otros usuarios de Internet (Asenjo, 2008); observando que los errores de configuración, que pueden generar vulnerabilidades operacionales y de seguridad, se deben enfocar en las dos propiedades de la configuración de DNS que se necesitan mantener, tanto en la lógica como en el nivel físico: la coherencia, donde si una entidad DNS es declarada en múltiples lugares, ya sea a nivel físico o lógico, todas las declaraciones deben ser coherentes; y la independencia en la cual, si dos entidades DNS, declaradas en el nivel físico o lógico, son distintas, entonces deben ser independientes entre sí (Vasileios, 2004).

Con el fin de documentar estas y muchas otras vulnerabilidades, desde 1997 el US-CERT[2] (*United States Computer Emergency Readiness Team)* ha publicado decenas de documentos donde se describen diferentes aspectos de vulnerabilidades, en áreas como el DNS, ataques a servidores, problemas de seguridad y configuración, etc., detectados, sufridos y/o solucionados en diferentes organizaciones de Estados Unidos y el mundo.

Para contextualizar el panorama de esta temática, en este artículo se presentan las siguientes secciones: en la sección III se caracteriza al DNS en el ámbito de los sistemas distribuidos, la sección V se enfoca en la revisión de los principales aspectos de seguridad de DNS, la sección VI se orienta a las vulnerabilidades en seguridad más relevantes que se pueden presentar en este tipo de sistemas y posteriormente en la sección VII se expondrán las técnicas más reconocidas actualmente para afrontar este tipo de vulnerabilidades de seguridad.

III. DNS como sistema distribuido

El sistema de nombres de dominio es una base de datos distribuida responsable de la traducción de nombres a direcciones de localizaciones de red, y su funcionalidad es un componente crítico para casi todas las aplicaciones de red, incluida la navegación en la Web y correo electrónico. Dentro de sus servicios se definen[3]:

1. Un espacio de nombres jerárquico para los hosts y las direcciones IP.

[1] http://dns.measurement-factory.com/surveys/sum1.html
[2] http://www.us-cert.gov/
[3]http://www.virtuniversidad.com/manual/seguridad/VUrouter_dns.html

2. Una tabla de hosts implementada como una base de datos distribuida.
3. Un traductor (del inglés, resolver) o librería de rutinas que permite realizar consultas a esa base de datos.
4. Enrutamiento mejorado para el correo electrónico.
5. Un mecanismo para encontrar los servicios en una red.
6. Un protocolo para intercambiar información de nombres.

Para comprender este contexto de distribución es prudente revisar muy rápidamente el proceso de una búsqueda de nombre, proceso que funciona según los explica Pang (2004), de la siguiente manera: una consulta es ejecutada por el resolver del cliente, una librería implementada por el protocolo DNS sobre la máquina del usuario. Esta petición es enviada al servidor DNS local (LDNS), que regularmente suele ubicarse dentro de la organización del usuario y que adquieren suma importancia al almacenar en caché los registros DNS ejecutados anteriormente. Al no tener respuesta, los servidores LDNS consultan iterativamente los servidores DNS autoritativos para tratar de solventar las solicitudes de nombres del usuario, consultando en primera instancia al servidor raíz, y posteriormente uno a uno los servidores autoritativos adicionales.

Como se observa en el proceso de consulta, ésta base de datos DNS se distribuye a través de la jerarquía de servidores autoritativos DNS (ADNS), ubicándose en la parte superior de esta jerarquía el servidor raíz y los servidores de dominio de nivel más alto, los cuales mantienen los registros de ubicación de los servidores ADNS de nivel bajo en la jerarquía, que contienen los registros de nombre – dirección, que permiten resolver de forma recursiva, la consulta planteada por el usuario.

Esta comunicación con la base de datos DNS sigue el paradigma cliente / servidor. El árbol de nombres de dominio se divide en zonas, las cuales por lo general son partes contiguas de los árboles. Estas zonas son definidas a través del proceso de delegación, que asigna a alguna organización la responsabilidad de gestionar subdominios particulares, por ende, una zona puede contener información acerca de un dominio y sus subdominios (Ateniese et al., 2001).

Para asegurar la disponibilidad de DNS, Pappas et al.(2004) plantean dividir los elementos de infraestructura de DNS en dos clases: los elementos a nivel físico, tales como los servidores de nombres, y los elementos a nivel lógico, tales como la infraestructura de almacenamiento de datos DNS llamada Registro de Recursos (RR). De la misma forma también se deben identificar dos propiedades principales en la configuración DNS que son necesarias mantener permanentemente, tanto en la lógica como en el plano físico, para que una configuración sea correcta y poder mantener la disponibilidad del servicio: la coherencia en la declaración de entidades y la independencia entre ellas.

IV. La seguridad en DNS

Como lo describe Chandramouli (2006), la confiabilidad, la integridad, la disponibilidad y la autenticación de las fuentes son los objetivos de seguridad comunes en cualquier sistema distribuido, sin embargo, de DNS se espera que proporcione la información de resolución de nombres para cualquier recurso disponible públicamente en Internet. Con excepción de los datos DNS de los recursos internos (por ejemplo: servidores antes de firewalls), los cuales son proporcionados por servidores de nombres DNS internos a través de canales seguros, los datos de DNS provistos por servidores de nombres públicos no se consideran confidenciales. Por lo tanto, la confidencialidad no es uno de los objetivos de seguridad de los DNS.

El aseguramiento de la autenticidad de la información y el mantenimiento de la integridad de la información en tránsito son los servicios críticos para el funcionamiento eficiente de la Internet, por lo cual DNS proporciona el servicio de resolución de nombres, convirtiendo así a la integridad y autenticación de fuentes en los principales objetivos de seguridad de DNS.

De la misma forma, se deben manejar aspectos de seguridad en la infraestructura DNS, clasificada bajo los siguientes parámetros:

- La plataforma DNS: El nivel de seguridad de las plataformas sobre las cuales corre el software DNS, depende de la configuración provista por el sistema operativo que la soporta.
- El software DNS: El nivel de seguridad ofrecido en este aspecto está ligado a factores como las versiones, el nivel de privilegios con los que se trabaje, las políticas y restricciones establecidas para el ambiente de computo y el tipo de dedicación soportada por las máquinas que prestan los servicios de DNS, entre otros factores que permiten otorgar características de seguridad al software.

- El control de contenidos de los archivos de zona: Debido a su característica distribuida, para controlar los contenidos de los archivos de zona, se usa un comprobador de integridad de los archivos de

zona, que depende de las restricciones cargadas en la bases de datos.

De otra parte, la seguridad en DNS se ve reflejada en las características de infraestructura proporcionadas (Pang, 2004), dentro de las cuales se pueden contemplar:

1. Distribución de carga: la cantidad de carga en cada uno de los servidores, entendida como el número de consultas que recibe, es un indicador de la cantidad de usuarios que acceden a él.
2. Disponibilidad: la disponibilidad de un servidor determina la frecuencia con la que será capaz de atender solicitudes de servicio.
3. El estilo de *deployment,* que se perfila hacia la forma como la organización ubica sus usuarios en su servidor local de nombres, o los distribuye a través de sus diferentes servidores.

Adicionalmente, según lo describe Pappas et al. (2004), un último factor a analizar dentro de los diferentes aspectos de seguridad en DNS es la configuración del DNS, debido al impacto que tiene, sobre la disponibilidad de los servicios de zonas DNS y el rendimiento del sistema, cualquier decisión tomada en la configuración de una zona especifica. Algunos resultados de evaluar el factor de configuración sobre los servicios DNS se pueden observar en estudios como *Impact of Configuration Errors on DNS Robustness,* realizado por Pappas et al. (2004), del cual se pueden observar resultados como que el 15% de las zonas DNS sufren específicamente de un mix de configuración llamado *lame delegation*, en el cual una zona padre direcciona un servidor de nombres erróneo a una zona hija; por lo cual, la configuración adquiere relevancia dentro de los procesos de seguridad en los ambientes DNS.

V. Vulnerabilidades de Seguridad en DNS

Después de revisar muy rápidamente los principales factores de seguridad en los sistemas DNS, es conveniente tratar las principales vulnerabilidades de seguridad presentadas en estos sistemas, donde algunas de estas vulnerabilidades se derivan, entre otras causas, de malas o inadecuadas prácticas de aseguramiento de los servicios DNS.

Tal como lo describe Radack (2006), el DNS es susceptible a muchas de las mismas vulnerabilidades que los demás sistemas de computación distribuida. Estas vulnerabilidades incluyen la plataforma, el software, y los niveles de red, así como también aplican para la mayoría de los sistemas distribuidos, los objetivos de seguridad de confidencialidad, integridad y disponibilidad de información:

- Una pérdida de la confidencialidad es la divulgación no autorizada de información.
- Una pérdida de la integridad es la modificación no autorizada o la destrucción de información.
- Una pérdida de la disponibilidad es la interrupción del acceso o uso de información o de un sistema de información.

Adicionalmente, debido a que DNS maneja un sistema de infraestructura para Internet, posee unas características especiales a diferencia de otros sistemas distribuidos, tales como no tener límites definidos, debido que no hay limitaciones en topología o ubicación geográfica; y no se requiere confidencialidad en los datos debido a que los datos DNS son públicos, pudiendo ser accesibles por cualquier entidad independiente de su ubicación.

Enmarcado en este contexto, a continuación se presentan algunas de las más importantes vulnerabilidades de seguridad que se presentan en DNS:

VI. Vulnerabilidades de seguridad que se presentan en DNS

1. En el flujo de datos

En la figura 1, Bellido y Fernández (2007) describen las principales vías de ataque al servicio DNS en el contexto de todos los flujos de datos, donde se puede apreciar que la seguridad del sistema en su conjunto debe comprender tanto la protección de las transacciones entre servidores como la integridad en tránsito de los datos hacia los clientes.

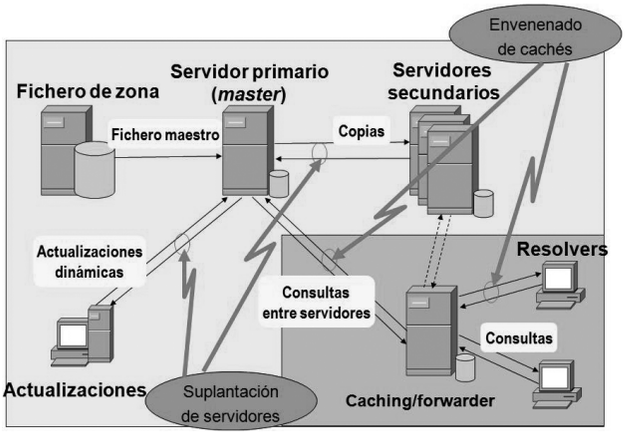

Figura 1. *Vulnerabilidades en Flujo de Datos DNS. Fuente: Bellido y Fernández (2007)*

Según como lo describe tech-faq[4], Adrian, Díaz (2003) y Hernández (2006), los ataques a los flujos de

datos en DNS se pueden clasificar globalmente como:

· Suplantación: Los servidores DNS que responden consultas en modo recursivo son vulnerables a un ataque del tipo de suplantación de respuestas. En este ataque, el servidor DNS es engañado haciéndole creer que está recibiendo una respuesta desde un servidor DNS de confianza. El suplantador realiza alguna acción que tiene el efecto de cambiar la dirección IP de un cierto nombre de dominio por una dirección IP de su propia elección. Una vez que el servidor DNS engañado ha almacenado una incorrecta traducción entre un nombre de dominio y una dirección IP, el suplantador puede falsear las operaciones que se hagan sobre el nombre que ha sido "secuestrado".

· Envenenado de Caches: Si un servidor DNS es engañado y el parámetro "Time To Live" asociado con la información falsa es establecido por el suplantador en un valor alto, la información comprometida permanecerá en la caché, esperando a ser requerida en el momento que se responda a una consulta del nombre de dominio asociado al dato comprometido.

· Ataques de negación de servicio (DoS y DDoS): se producen cuando los servidores DNS están inundados con peticiones recursivas[5]. Un exitoso ataque de denegación de servicio puede dar lugar a la falta de disponibilidad de los servicios de DNS, y en el eventual apagado de la red.

· Piggy in the middle: Se presenta cuando el atacante puede hacer sniffer sobre el tráfico de la red usada por DNS, interceptando los paquetes DNS y utilizando esta información para atacar poniéndose en medio entre el resolver y el servidor de nombres, asumiendo la identidad del servidor e interceptando las consultas enviadas al servidor.

En conclusión, la revisión de las vulnerabilidades de seguridad del sistema DNS en su conjunto no solo se limita a la protección de las transacciones entre servidores, sino que se extiende a la integridad del flujo o tránsito de los datos hacia los clientes, como se muestra en la figura 2 (Castro, 2005):

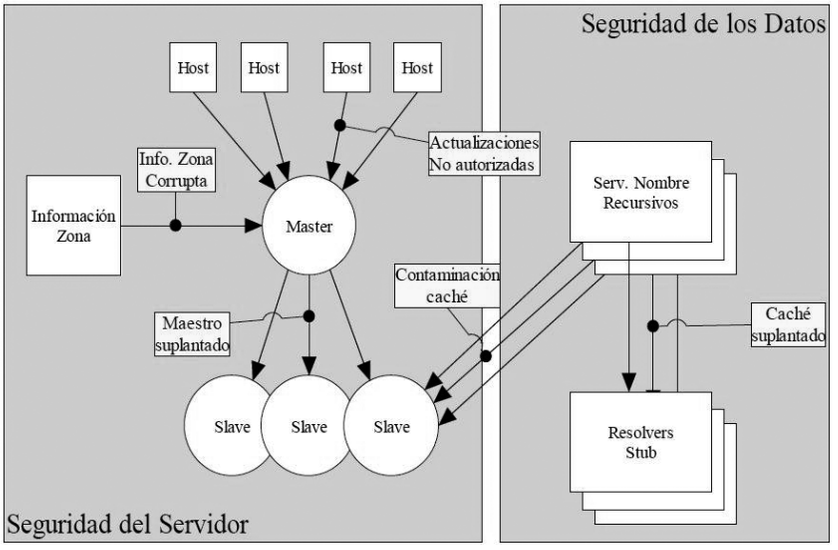

***Figura 2**. Vulnerabilidades DNS. Fuente: Castro, 2005*

2. Errores de configuración DNS

Según Radack (2006), la infraestructura DNS está compuesta de protocolos de comunicación, diferentes componentes DNS (navegadores, servidores, etc.), políticas que rigen la configuración de esos componentes y los procedimientos de creación, almacenamiento y uso de nombres de dominio. Por ello, un error en la configuración de algunos de ellos puede producir grandes vulnerabilidades de seguridad, además de problemas de disponibilidad y desempeño.

Las decisiones locales en la configuración de una determinada zona DNS, por ejemplo, pueden tener repercusiones negativas a nivel mundial en robustez y rendimiento, de aquí la relevancia de identificar las principales vulnerabilidades presentadas en la configuración DNS.

Según Pappas et al. (2004), en su artículo Distributed DNS Troubleshooting, se deben contemplar dos propiedades de la configuración de DNS que se necesitan mantener, tanto en la lógica como en el nivel físico, con el fin de lograr una configuración correcta, las cuales son:

Coherencia: que se refleja en que si una entidad DNS es declarada en múltiples lugares, ya sea en el ámbito físico o lógico, todas las declaraciones deben ser coherentes.

Independencia: que se observa en que si dos entidades DNS, declaradas en el nivel físico o lógico, son distintas, entonces deben ser independientes entre sí. Por ejemplo, dos nombres de servidores distintos, que son autorizados por

[4] www.tech-faq.com
[5]http://apps.extremenetworks.com/libraries/whitepapers/technology/Security_Defending_WP.asp

la misma o incluso diferente zona, son entidades DNS declaradas tanto en el ámbito físico como lógico.

La violación de cualquiera de estas dos propiedades puede reducir la disponibilidad del sistema DNS. La violación de la coherencia reduce el número de servidores redundantes incondicionalmente, lo que significa que el número de servidores disponibles es más bajo que el esperado, por el contrario, una violación de independencia reduce el número de servidores redundantes condicionalmente, lo que significa que el número de servidores disponibles es más bajo de lo esperado, solo cuando ciertas condiciones son verdaderas, como cuando un servidor no está disponible.

De igual forma en un artículo posterior, Pappas et al. (2004) expone posibles errores de configuración que pueden ser catalogados como violaciones a las propiedades de coherencia o independencia, dentro de las cuales se consideran:

· Lame Delegation, que ocurre cuando un servidor de nombres, que está registrado en el sistema DNS, como autoritativo para una zona, no proporciona respuestas autoritativas para dicha zona, situación que puede ocurrir cuando el servidor DNS corre sobre una máquina no registrada, o cuando el servidor corre sobre una máquina registrada pero no tiene datos autoritativos o responde con errores de localización.

  Este tipo de error causa dos grandes problemas, uno es que el número de servidores disponibles para la zona puede ser mucho más bajo que el indicado en la configuración, lo cual da una falsa percepción del nivel de redundancia de la zona; el otro es que incrementa el tiempo de respuesta para las consultas, ya sea en la misma o entre zonas.

· Dependencia Cíclica de Zona, ocurre cuando para resolver una zona Z1, el resolver necesita consultar una zona Z2, la cual para ser resuelta requiere que la zona Z1 sea resuelta primero. En otras palabras, las zonas Z1 y Z2 dependen una de la otra de forma recíproca.

  En Spring (2006) se argumenta que identificar este tipo de errores en las zonas es complejo debido a que los ficheros de configuración no presentan errores aparentes, y en condiciones normales cuando todos los servidores están disponibles, los servidores que forman la dependencia parecen estar disponibles, y presentan la problemática.

· Disminución de la configuración de redundancia de servidor, ocurre cuando dos o más servidores, que son autoritativos para la misma zona, son ubicados de manera tal que una falla en un componente puede causar la falla de estos servidores. Por ejemplo, colocar estos servidores detrás de un mismo router puede sacarlos de la red si el router falla, o si utilizan el mismo prefijo de red, pueden quedar fuera si existen problemas de enrutamiento.

Por otra parte, una encuesta llevada a cabo por The Measuremente Factory[6] y patrocinada por Infoblox[7], permite establecer otras vulnerabilidades enmarcadas como errores de configuración DNS, dentro de las cuales se tiene:

- Servicios de Recursividad: Entre el 75 y el 84% de los DNS investigados[8] proporcionaban servicios de recursividad a peticiones arbitrarias de Internet. Las buenas prácticas de la industria dictan que los servicios de recursividad de DNS deben sólo ser permitidos para una lista restringida de demandantes conocidos y de confianza. Proporcionando recursividad a direcciones arbitrarias IP en Internet expone al DNS a ataques de denegación de servicio.
- Transferencia de Zonas: Más de 40% de los DNS investigados proporcionan transferencia de zona a peticiones arbitrarias. Como los servicios recursivos del DNS, las transferencias de zona, que copian un segmento entero de datos DNS de una organización desde un servidor DNS a otro, deben únicamente permitirse para una lista de hosts fiables y autorizados tales como DNS secundarios. Ofrecer transferencias de zona a cualquier petición supone exponer a los DNS a ataques de denegación de servicio.
- Configuración de segmentos: Casi una tercera parte de los DNS que han sido instalados para proporcionar redundancia para datos jerárquicos, son configurados en el mismo segmento de red IP. Como resultado, un exitoso ataque de denegación de servicio en un único segmento de red o una caída de una porción de red puede resultar en una pérdida de servicios autorizados, eliminando los beneficios de instalar servidores DNS múltiples y redundantes.

En síntesis, cualquier problema en los procesos de configuración, por mínimo que este sea, ya sea por malas prácticas, descuido, desconocimiento, etc., puede producir vulnerabilidades de seguridad que atentan contra la disponibilidad de los recursos del sistema, rendimiento de los mismos, tiempos de respuestas de resolución de las consultas realizadas, etc.

[6] http://www.measurement-factory.com/
[7] http://www.infoblox.com/
[8] http://www.seguridad0.com/index.php?ID=2169

3. Otros tipos de vulnerabilidades

Otros aspectos importantes que son catalogados como vulnerabilidades de seguridad en DNS con respecto a errores de configuración, según lo que plantea Asenjo (2008) corresponden a problemáticas como:

· Configuración de servidores recursivos. Este tipo de configuraciones en la arquitectura DNS permite que los servidores DNS reenvíen peticiones procedentes de sistemas fuera de su propia red, es decir, son "recursivos". Visto de otra forma, los servidores que residen en una LAN se comunican con sus respectivos servidores autorizados, enviando las consultas a ejecutar. Mientras las consultas se mantengan dentro de la red el problema es inexistente, pero se activa cuando dichas consultas salen de la red local, quedando expuestas a diferentes ataques descritos anteriormente.

· El manejo de operaciones de transferencia de zona sin ningún tipo de restricción o actualización de los servidores secundarios mediante la descarga de la información de la zona, desde el servidor primario, plantea una carta abierta para que cualquier intruso tome información de esta transferencia y produzca diferentes tipos de ataque a la infraestructura y al flujo de datos. Para Bellido (2007), la restricción de las transferencias de zona es un paso importante en el aseguramiento de un servidor, protegiendo el listado de los contenidos de una zona. Pero una vulnerabilidad fuerte consiste en restringir las transferencias de zona desde los servidores primarios pero olvidarse de hacerlo en los secundarios.

· Actualización dinámica del DNS. Los protocolos como Dynamic Host Configuration Protocol (DHCP) hacen uso de protocolos de actualización dinámica DNS para adicionar y eliminar registros de recursos por demanda, llevándose a cabo en el servidor primario de la zona. Las autenticaciones de estas actualizaciones están basadas en la dirección IP de origen y son vulnerables a diferentes amenazas (Ariyapperuma, 2007).

· Manejo de versiones de software desactualizadas, inseguras o mal configuradas. No tener actualizada la plataforma de software que soporta los procesos del sistema DNS, o que administran las máquinas donde este se ejecuta representa un gran punto de vulnerabilidad en seguridad. De la misma forma, la mala asignación de privilegios, la deficiente configuración de servicios como los firewall, entre otros, abren puertas por donde se puede filtrar cualquier amenaza al sistema.

Por su naturaleza distribuida, DNS afronta este tipo de problemáticas debido a aspectos como contar con configuraciones heterogéneas, geográficamente dispersas, que no conservan uniformidad en las instalaciones y configuraciones que manejan, distribución jerárquica de los registros de recursos, entre otros factores, que comprometen la seguridad del sistema.

VII. Principales técnicas / recomendaciones de seguridad utilizadas

Después de haber planteado las principales vulnerabilidades de seguridad en DNS, esta sección se enfoca en revisar las principales técnicas utilizadas para prevenir o contrarrestar este conjunto de vulnerabilidades de seguridad presentes en DNS, las cuales a continuación se presenta en la siguiente clasificación:

1. Asegurando el DNS

Con el fin de asegurar la infraestructura DNS, instale un servidor perimetral o red externa de DNS y otro para la red interna, de tal forma que cualquier consulta externa será atendida por el servidor perimetral, sin afectar de frente la estructura interna del sistema DNS[9], mientras que el servidor interno respalda la resolución de nombres a nivel LAN permitiendo mantener actualizado y seguro el esquema direcciones IP's sin tener consultas recursos externos[10]. Visto de otra forma, el principio consiste en dividir el sistema en dos partes, lo que se denominaría Arquitectura DNS Split, donde una parte es responsable de la publicación del mapeo de nombre – dirección, y la otra resuelve los requerimientos internos, es decir, con los que se tenga "relación de confianza", entendida esta dentro del contexto de seguridad de sistemas distribuidos, como una respuesta a los inadecuados mecanismos de autorización (Blaze, 2000; Carli, 2003).

De la misma forma, para proteger la transferencia de zonas especifique la IP de los servidores de DNS que participan en la transferencia de zonas, de esta manera se limita a dichos servidores el acceso y la replicación. Aunque esta técnica restringe el acceso a la transferencia de zona, no protege los paquetes que están viajando en la transferencia. Para ello, encripte el tráfico DNS utilizando IPSec.

Otra medida general de seguridad consiste en distribuir servidores y utilizar distintas máquinas con distintos roles en una misma organización. Así es posible diseñar distintas políticas de seguridad de manera

[9] Networks., E. (s.f.). Solutions Brief : Approach to Information Security Solution Brief

[10] http://www.creangel.com/drupal/?q=node/128

que si un servidor queda comprometido, un segundo seguirá proporcionando el servicio con normalidad. Pero para combatir ataques por DoS y prevenir discontinuidades en el servicio, es importante que se eliminen puntos únicos de fallo en la infraestructura del DNS. Para ello se debe evitar ubicar todos los servidores DNS de una organización en una misma subred, o detrás de un mismo router e incluso dentro del mismo sistema autónomo (Bellido et al., 2007).

Igualmente, si su servidor solo maneja DNS en su plataforma, restrinja las reglas del firewall para que permita tráfico DNS por el puerto 53[11]. Ya que las transferencias de zona trabajan con TCP, el router podría restringir a solo tráfico TCP por el puerto 53 proveniente de los servidores de nombres esclavos. Haciendo esto se estaría colocando una capa de seguridad que restringiría las transferencias de zona a servidores autorizados (Teoh, 2003).

2. El software y los datos DNS

La plataforma sobre la cual corre el software DNS debe estar debidamente asegurada, pero como se enfrenta a la problemática de heterogeneidad, se deben tener en cuenta estrategias como:

Como ocurre con cualquier software que sea accesible a través de la red, es crítico mantener actualizado el software de DNS con la última versión. Las versiones antiguas suelen tener agujeros de seguridad muy conocidos. El instalar la última versión del software no garantiza una seguridad total, pero minimiza las posibilidades de ataque.

Ejecute la última versión del software de servidor de nombre, como por ejemplo BIND, asegurándose así de actualizarse contra las últimas vulnerabilidades encontradas en el sistema. Desactive la versión de consulta, que por ejemplo en BIND (Albitz, 2001) retorna el número de versión del demonio del servidor, información que permitiría clasificar ataques a ejecutar sobre la infraestructura.

Ejecute el software de servidor de nombres con privilegios restringidos, es decir como usuario sin privilegios con acceso restringido a directorios específicos. Aísle el software DNS, asegúrese de no correr sobre la misma plataforma otro tipo de herramientas del sistema operativo o de soporte de red (Chandramouli et al., 2006; Hinshelwood, 2003), 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 asegurado al nivel de sistema operativo[12]. Igualmente dentro de las recomendaciones también se contempla instalar los servidores primarios y secundarios en plataformas de software distintas, con el fin de aumentar el nivel de dificultad ante los ataques (Holmblad, 2009).

3. Las transacciones DNS

En cuanto a las transacciones manejadas por el sistema DNS, se presentan las siguientes técnicas:

Restrinja las transacciones basadas en direcciones IP. Esta técnica se basa en delimitar los clientes y servidores que participan en las transacciones DNS, restringiendo el acceso a un conjunto de direcciones debidamente autorizadas. Aunque la ejecución de esta técnica previene ataques de tipo spoofing, no es recomendada en DNS query/response, transferencias de zona y transacciones de actualización dinámica que manejen alto impacto en el sistema, es decir, que involucren grandes cantidades de recursos distribuidos en la red. De igual forma, proteja las transacciones utilizando la especificación TSIG, que opera a través de la generación y verificación de códigos de autenticación de mensajes de base hash (HMAC) (Chandramouli et al., 2006).

Para implementar estas técnicas, utilice DNS Seguro – DNSSEC -, que corresponde a la primera RFC sobre aseguramiento de DNS, publicada en 1997. El objetivo del DNSSEC consiste en proveer autenticación e integridad para los datos recibidos desde una base de datos DNS. La idea general es que cada nodo en el árbol DNS es asociado con una llave pública, cada mensaje del servidor DNS es firmado con la correspondiente llave privada (Ateniese et al., 2001; Cachin, 2004).

Esta técnica busca ofrecer mecanismos de: autenticación de servidores, a través de medios como TSIG (Transaction Signatures) que es un protocolo que permite el intercambio seguro de la información contenida en los ficheros de zona, de este modo es posible asegurar la veracidad de los datos contenidos en los servidores, previniendo ataques de suplantación de servidores en actualizaciones o en transferencia de zonas; y mecanismos para integridad de datos y autenticación utilizando criptografía de llave públi-

[11] http://www.spirit.com/Network/net0600.html

[12] http://www.hacktimes.com/?q=node/27

ca y firmas digitales, previniendo así el envenenado de caches en consultas y respuestas. (Bellido et al., 2007; Castro, 2005; Díaz, 2003).

Existen diversas alternativas sobre la restricción de consultas recursivas dependiendo de las necesidades y requisitos de la organización y de la arquitectura de servidores elegida (Radack, 2006), dentro de las cuales se recomienda:

- Siempre deshabilitar la recursión, es decir, la capacidad de un servidor DNS de consultar a otros cuando no tiene en sus registros una información de los servidores DNS que no requieren de esta función, el servidor nunca enviará consultas, adoptará un modo pasivo y no almacenará nada en su caché. Esto limita la eventualidad de ataques de contaminación de caché o vulnerabilidades que necesitan de su presencia para la explotación, o simplemente la posibilidad de que terceros empleen el servidor DNS para sus resoluciones (Hernández, 2006). Puede no ser solución aceptable cuando hay resolvers o servidores que necesitan recursión y no hay medio de distribuir el servicio.

- Restringir las consultas que un servidor acepta desde los resolvers (allow-query)[13]. Cualquiera puede preguntar por datos en zonas sobre las que este servidor tenga autoridad, pero sólo los resolvers "internos" pueden preguntar por datos en zonas externas.

De igual forma, evite el uso de la caché DNS: por ejemplo BIND (Bawer 2000), 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.

VIII. Conclusiones

· Los servicios de resolución de nombres en Internet, brindado por DNS, lo convierte en uno de los sistemas más indispensables, pero a la vez más críticos debido a aspectos que ponen en riesgo su infraestructura, información, integridad y consistencia, tales como que su diseño se basa en servidores redundantes, los datos de DNS provistos por sus servidores son de manejo público y no se consideran confidenciales, entre otros aspectos, que unido a su naturaleza distribuida, DNS no es ajeno de afrontar diferentes problemáticas de escalabilidad, transparencia, heterogeneidad y de seguridad, más aún cuando los datos manejados por DNS están destinados a ser de dominio público, y su infraestructura inicial no contemplaba la definición de una alta seguridad.

· Uno de las principales problemáticas de seguridad, además de los virus, spoofing, etc., corresponde a las inconsistencias y mezclas de configuraciones existentes, es decir, heterogeneidad de configuración, plataformas, políticas y demás, presentes en su ambiente distribuido, que lo hacen vulnerable a errores que no solo afectan su desempeño y disponibilidad, si no la integridad y consistencia de la información que maneja. Anotando que este tipo de vulnerabilidades se presenta como resultados de procesos humanos, es conveniente tomar las precauciones necesarias y aplicar todas las recomendaciones existentes, a fin de mitigar los riesgos presentados en la estructura DNS.

IX. Referencias

[1] Adrian, A., Álvarez, L., Méndez, A. & Varona, J. (s.f.). *Seguridad en Internet: una clasificación.* Recuperado el 2 de Febrero de 2008, de http://ldc.usb.ve/~figueira/Cursos/redes2/EXPOSICIONES/SeguridadInternet/resumen.html

[2] Albitz, P. & Liu, C. (2001.). *DNS and BIND*. 4th Edición.

[3] Ariyapperuma, S., & Mitchell, C. J. (2007). Security vulnerabilities in DNS and DNSSEC *Availability, Reliability and Security*. The Second International Conference on Volume , Issue.

[4] Asenjo, A. (2008). *Las mejores prácticas para DNS.* Obtenido de NetworkWorld, Comunicaciones World. Recuperado el 17 de Marzo de 2008, de http://www.idg.es/comunicaciones/articulo.asp?id=184261

[5] Ateniese, G. & Mangard, S. (2001). *A New Approach to DNS Security* (DNSSEC). Philadelphia, Pennsylvania, USA: Copyright 2001 ACM 1-58113-385-5/01/0011.

[6] Bauer, M. D. (2000). Securing DNS and BIND. *Linux Journal*

[7] Bellido, L. & Fernández, D. (2007). Introducción a la tecnología DNS. *Departamento de ingeniería de Sistemas Telemáticos* . ETSIT UPM.

[8] Blaze, M. (2000). The Role of Trust Management in Distributed Systems Security. *Network Security Library. WindowSecurity.com.*

[9] Cachin, C. S. (2004.). Secure distributed DNS. Ruschlikon, Switzerland: ISBN: 0-7695-2052-9. IEEE.

[10] Carli, F. (2003). Security Issues with DNS. *SANS GSEC Practical Assignment*. SANS Institute.

[11] Castro, S. (2005). *Encuentro Open Source y nue-*

[13] http://www.virtuniversidad.com/manual/seguridad/VUrouter_dns.html

vas tecnologías: Extensiones de seguridad para el DNS. UCENTUX.
[12] Chandramouli, R. & Rose, S. (2006). Challenges in securing the domain name system. *US Nat. Inst. of Stand. & Tecnology* . Gaithersburg, MD., USA: Jan.-Feb. 2006 Volume: 4 , ISSN: 1540-7993. IEEE.
[13] Chandramouli, R., & Rose, S. (2006). Secure Domain Name System (DNS) Deployment. *Guide Recommendations of the National Institute of Standards and Technology. Computer Security Division Information Technology. Laboratory National Institute of Standards and Technology* Gaithersburg, MD 20899-8930.
[14] Díaz, G. (2003). Capa de Transporte. *Universidad de Los Andes, Facultad de Ingeniería, Escuela de Sistemas* . Mérida, Venezuela.
[15] Factory., T. M. (s.f.). *Domain name servers: pervasive and critical, yet often overlooked.* Obtenido de http://dns.measurement-factory.com/surveys/sum1.html
[16] Farrow, R. (s.f.). *TROUBLE WITH DNS*. Obtenido de http://www.spirit.com/Network/net0600.html
[17] Hernández, M. Á. (2006). Riesgos en el Sistema DNS: Vulnerabilidades. SIC No 68 , 96 -98.
[18] Hinshelwood, D. (2003). DNS, DNSSEC and the Future. *GSEC Paper Practical Assignment Version 1.4b.* SANS Institute.
[19] Holmblad, J. (2003). The evolving to the availability and security of the Domain Name Server. *SANS GIAC/GSEC Practical*. SANS Institute.
[20] Kaminsky, D. (2003). Attacking Distributed Systems: The DNS Case Study. Avaya.
[21] Networks., E. (s.f.). *Approach to Information Security: Defending Against Network-Based Attacks.* Obtenido de White Papers Extreme Networks®: http://apps.extremenetworks.com/libraries/whitepapers/technology/Security_Defending_WP.asp
[22] Networks, E. (s.f.). *Solutions Brief : Approach to Information Security Solution Brief.* Obtenido de http://apps.extremenetworks.com/libraries/casestudies/Security_SB.asp
[23] Pang, J. & Otros. (2004). *Availability, Usage, and Deployment Characteristics of the Domain Name System.* Taormina, Sicily, Italy: Copyright 2004 ACM 1581138210/04/0010.
[24] Radack, S. (2006). Domain Name System (DNS) Services: NIST recommendations for secure deployment. *Computer Security Division Information Technology Laboratory.* ITL Bulletin : National Institute of Standards and Technology Technology Administration.U.S. Department of Commerce.
[25] Seguridad0.com. (2005). *El 84 por ciento de los servidores dns de todo el mundo son vulnerables a ataques pharming.* Recuperado el 3 de Marzo de 2009, de http://www.seguridad0.com/index.php?ID=2169
[26] Spring (2006) Automation Will Solve Most of Our Problems. CS553: Internet Services,
[27] tech-faq., T. (s.f.). *Obtención de DNS*. Recuperado el 5 de Febrero de 2009, de http://www.tech- faq.com/lang/es/securing-dns.shtml
[28] Teoh, C. (2003). Defense in Depth for DNS. *GSEC Version 1.4b* . SANS Institute.
[29] Vasileios, P., Patrik, F., Daniel, M., Lixia, Z.. (2004). Distributed DNS Troubleshooting. *SIGCOMM'04 Workshops* . Portland, Oregon, USA.: Copyright 2004 ACM 158113942X/04/0008.
[30] Vasileios, P., Patrik, F., Daniel, M., Lixia, Z.. (2004). Impact of Configuration Errors on DNS Robustness. *SIGCOMM'04* . Portland, Oregon, USA. : Copyright 2004 ACM 1581138628/04/0008.
[31] Virtuniversidad. (2004). *El sistema de nombres de dominio*. Obtenido de http://www.virtuniversidad.com/manual/seguridad/VUrouter_dns.html

Jhon Francined Herrera C. *Ingeniero de Sistemas, Especialista en Alta Gerencia, Especialista en Construcción de Software para Redes. Magíster en Ingeniería de Sistemas y Computación, Universidad de los Andes (UNIANDES). Docente tiempo completo del programa de Tecnología en Informática, Corporación Universitaria Minuto de Dios (UNIMINUTO), jherrera@uniminuto.edu*