Riesgos en el sistema de DNS

El sistema DNS juega un papel esencial en la infraestructura de Internet. Prácticamente cualquier servicio que podamos utilizar realiza como paso previo a una comunicación la resolución de los nombres de *host* de las máquinas con las que vamos a conectar. Pese a todo, este protocolo es uno de los grandes olvidados en el diseño de infraestructuras y soluciones de seguridad. Actualmente, las vulnerabilidades de sistemas operativos o de modernas tecnologías como los servicios web, comunicaciones inalámbricas, etc., acaparan toda la atención. Sin embargo, las amenazas que suponen las vulnerabilidades DNS permanecen latentes y pueden subvertir el modelo de seguridad de la mayoría de aplicaciones actuales.

Miguel Ángel Hernández Vallejos

ANTECEDENTES

En los inicios de Internet, durante la década de los 70, la asignación de nombres a IP´s se realizaba por medio de ficheros de *hosts* estáticos, primero locales y luego versiones centralizadas, que se podían descargar por FTP. Cuando a principios de los 80 quedó patente que este sistema era poco práctico, se diseñó un protocolo específico para estas tareas: el Domain Name System **[1]**.

El sistema DNS se puede definir como una base de datos distribuida y jerárquica que contiene las relaciones entre nombre de *host* e IP, además de contener información adicional como son los registros MX. La versión que usamos actualmente es poco más que una actualización de las bases que se sentaron en el RFC 882 en noviembre de 1983. Al igual que ha ocurrido con otros protocolos que se diseñaron en los primeros tiempos de Internet: IPv4, SMTP, etc., raramente se incluían medidas de seguridad como la autenticación o confidencialidad, que tuvieron que ir añadiéndose *a posteriori* por medio de extensiones. Hoy en día ampliaciones del protocolo como DNSSEC **[2]** intentan remediar algunas de las vulnerabilidades, si bien su implantación en Internet es escasa.

AMENAZAS

El sistema DNS puede ser explotado por un atacante de múltiples formas. En sus vertientes más benignas puede ser utilizado como una valiosa fuente de información para ataques posteriores. Pero los mayores peligros vienen de la capacidad de explotar fallos en el protocolo o la implementación del mismo en clientes y servidores para conseguir modificar fraudulentamente las resoluciones de DNS, con el propósito de desviar las conexiones de sus destinatarios reales. A continuación enumeraremos cada una de estas amenazas que incluyen las referencias oportunas a artículos y herramientas disponibles en Internet para el lector que quiera profundizar en las mismas.

Obtención de Información

El paso previo a cualquier ataque informático contra una organización concreta (y por tanto, también de las auditorías del tipo *hacking* ético) consiste en identificar el mayor número posible de sistemas de la misma, su tipo y su funcionalidad. Cuanto mayor sea el numero de máquinas localizadas más fácil será que alguna de ellas se encuentre afectada por una vulnerabilidad. Para ello, un atacante puede usar en su provecho el sistema DNS.

El primer paso normalmente será emplear el comando Whois. El intruso obtendrá los DNS primario y secundario para los dominios de la organización objeto del ataque sobre los que podrá realizar diversas comprobaciones.

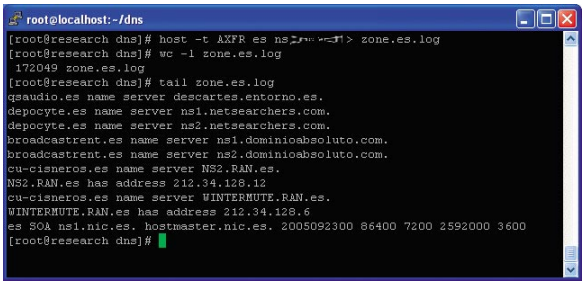

Figura 1

El más clásico de estos ataques consiste en la transferencia de zona (también conocido como AXFR). Usualmente utilizado para la replicación de datos entre servidores DNS, consiste en la solicitud al servidor DNS de todos los registros para un dominio. En la actualidad este tipo de peticiones por seguridad suelen limitarse de tal forma que sólo los *hosts* que necesitan de esta información (normalmente los servidores DNS secundarios de la organización) puedan acceder a ella. Un error común consiste en limitar este tipo de peticiones sólo en el servidor DNS maestro y permitiéndolo en los secundarios. Como ejemplo, en la **figura 1** se puede observar cómo es posible realizar un volcado AXFR para la zona .es (todos los dominios registrados españoles), aun cuando nic.es no lo permite directamente en ninguno de sus servidores publicados, consultando a un servidor DNS que dispone de privilegios para replicar esta información y no limita las peticiones AXFR.

Otra técnica habitual consiste en la resolución inversa de todo el espacio de direcciones asignado a la organización atacada. De esta forma, la existencia de una resolución nos dará el nombre de una máquina, lo que puede indicar tanto que se trata de una dirección IP activa como su cometido.

Las técnicas anteriores son ampliamente conocidas por lo que la mayoría de organizaciones con presencia importante en Internet deshabilitan tanto las transferencias AXFR como la resolución inversa. En ese caso, todavía queda un último recurso: el ataque de diccionario. En éste se toma una serie de nombres comunes (p.e., webmail, webpruebas, desarrollo, proxy, etc.) y se intenta resolver su existencia dentro del dominio de la organización. Esta comprobación tiene la ventaja adicional de que puede descubrir *hosts* que se encuentran en rangos de IP no registrados a nombre de la organización, por ejemplo, por encontrase albergados en un ISP.

Una variante especial de los ataques de obtención de información consiste en el llamado "DNS-Snooping" **[3]** el cual aprovecha la funcionalidad de *cache* de los servidores DNS para determinar si un determinado nombre ha sido o no resuelto anteriormente. Esto nos permite deducir que existe algún tipo de comunicación entre los usuarios de dicho DNS y los sistemas cuyos registros se encuentran en la *cache* DNS. Recientemente, este tipo de ataques se ha utilizado para determinar el grado de extensión del software de gestión de derechos de autor en los CD de audio de Sony también conocido como el "Rootkit Sony". Una comprobación masiva sobre DNS de Internet **[4]** descubrió que más de medio millón de DNS tenían *cacheada* la resolución DNS del *host* de Internet usado como maestro.

DNS Spoofing

El DNS Spoofing engloba todas aquellas técnicas que tiene como finalidad alterar fraudulentamente las resoluciones DNS. Normalmente se pretende conseguir que un usuario conecte con un sistema controlado por el atacante para llevar a cabo ataques *Man-In-The-Middle* y así capturar o modificar la información en tránsito.

Este tipo de ataques tendría dos variantes principales: el *hijacking* de respuestas a peticiones DNS y el envenenamiento de *cache*.

En la primera, el atacante tiene acceso a la red local o al encaminamiento del tráfico hacia el DNS y puede, por tanto, falsificar la respuesta del mismo antes de que lo haga el servidor DNS auténtico. Este tipo de ataque requiere normalmente de acceso a la red local, lo que limita su ejecución a usuarios internos maliciosos, aunque también puede tener un impacto significativo en redes locales públicamente accesibles, como cyber-cafés, redes *wireless* abiertas, etc.

En el segundo caso, el atacante, explotando diversas vulnerabilidades en el protocolo o implementación específica del servidor DNS, es capaz de inyectar en la *cache* de DNS una resolución fraudulenta, de manera que sucesivas peticiones por parte de usuarios serán contestadas con la misma.

En los últimos meses este tipo de ataques ha resurgido para dar lugar a una nueva variante de *phishing*. Se trata del conocido como *pharming*, en el que los defraudadores contaminan la *cache* de servidores DNS de Internet para la resolución de nombres de conocidas entidades financieras. De esta forma, los usuarios de esos DNS son redireccionados sin conocimiento por su parte cuando intentan acceder a los dominios legítimos.

En particular, las últimas oleadas de *pharming* se basan en fallos conocidos desde hace varios años

pero que siguen afectando a algunas configuraciones como la inclusión de respuestas con registros adicionales. Esta funcionalidad permite que en una respuesta DNS se incluyan resoluciones para más de un *host*. Los atacantes solicitan al DNS víctima la resolución de un dominio que controlan y en su respuesta añaden la resolución DNS fraudulenta del *host* suplantado que acaba en la *cache* del DNS atacado. Las resoluciones fraudulentas suelen afectar a dominios ampliamente visitados (google.com, Microsoft.com, etc.) o sitios de banca electrónica, y tienen la finalidad de sustituirlos por otros que instalan software tipo *spyware* o simulan los sitios de banca correspondientes.

En Internet se encuentran disponibles herramientas que permiten comprobar y/o explotar fácilmente los diversos tipos de DNS Spoofing, Por ejemplo, la utilidad dnsspoof del paquete Dsniff **[5]** o la *suite* de auditoría DNS dnsa **[6]**.

DNS como transporte para ataques

En muchas ocasiones los cortafuegos u otras medidas de filtrado no suelen ser capaces de detener ataques de intrusos a máquinas protegidas, aunque sí suponen una traba para extender la intrusion. Para evitarlos, los intrusos pueden establecer túneles (el equivalente *hacker* de las VPN) que les permitan una mayor conectividad y a la vez disimular el tráfico del ataque. Estos túneles se suelen establecer sobre aquellos protocolos no filtrados. DNS suele ser uno de ellos, ya que en muchas ocasiones la resolución de nombres de Internet se encuentra disponible aun cuando otro tipo de salida no lo esté.

La variante más sencilla consiste en utilizar para la comunicación el puerto 53 UDP (el asignado a DNS) si bien herramientas más sofisticadas como OzzymanDNS **[7]**, son capaces de atravesar DNS internos y evadir cortafuegos del tipo "inspección de contenidos" al encapsular los datos sobre peticiones DNS válidas.

Este tipo de ataque (aparte del escenario indicado de intrusión) también permite la conexión a Internet en aquellas redes Intranet con fuertes restricciones, o más particularmente en HotSpot inalámbricos de pago que suelen permitir las resoluciones DNS en el funcionamiento de sus portales de captura, posibilitando el establecimiento por tanto de túneles DNS hasta *host* controlados por el atacante, que realizan la función de *proxy* y por tanto la conexión a Internet a través del túnel de forma gratuita **[8]**.

Vulnerabilidades en servidores de DNS

Al constituir el DNS un punto crítico en la infraestructura de sistemas de información de cualquier organización, éste será un objetivo prioritario para cualquier intento de intrusión. Si el sistema que alberga el servidor DNS realiza funciones adicionales como servidor web o de correo se aumentan las posibilidades de vulnerabilidades remotamente explotables y, por tanto, el riesgo de una intrusión exitosa.

Aun cuando los servidores DNS realicen únicamente esta función no se debe olvidar que este servicio, como cualquier otro, puede ser susceptible a fallos de programación, que pueden ir desde los típicos *buffer overflow*, *bugs* de formato, etc., a fallos en la implementación del protocolo DNS que facilitan algunos de los ataques indicados.

Figura 2

Sirva de ejemplo que el popular demonio DNS Bind se ha visto afectado a lo largo de varios años por diversas vulnerabilidades explotables remotamente **[9]**, algunas incluso utilizadas en los gusanos de Internet como "Lion" **[10]**. Afortunadamente, la aparición de estas vulnerabilidades condujo a un esfuerzo general por parte de los desarrolladores de Bind a prácticas de programación más seguras y el número de vulnerabilidades detectadas en los últimos tiempos en este paquete se encuentra en declive, como se puede apreciar en la **figura 2**.

DoS y DNS

Como es sabido, los ataques de denegación de servicio (DoS) son aquellos que tienen como objetivo el degradar o impedir la prestación de un servicio; en el contexto que tratamos en este artículo y dado el papel fundamental de DNS en cualquier aplicación, éste se convierte en un objetivo tentador. Si un atacante consigue invalidar la posibilidad de resolución de nombres, normalmente se perderá la posibilidad de establecer cualquier tipo de comunicación.

Este hecho se ve agravado por la naturaleza jerárquica de DNS, por la cual la denegación de servicio total de un nivel provocará la de todos los inferiores. Así pues, un ataque exitoso sobre los Root Server, los servidores raíz que están en el punto más alto de la jerarquía, provocaría eventualmente la caída de todo Internet tal como lo conocemos. Este escenario de ataque, de hecho, ya ha tenido lugar. En octubre de 2002 se produjo un intento de ataque de DoS a gran escala contra los trece servidores raíz **[11]**. Afortunadamente, su diseño de alta disponibilidad con medidas tales como la dispersión geográfica por todo el planeta limitó el saldo final del ataque a una pérdida de rendimiento prácticamente no apreciable por el usuario de Internet. Sin embargo, cabe preguntarse si la infraestructura de DNS a nivel menor como la de un país o una organización concreta hubiera podido hacer frente a un ataque de estas características.

Asegurar DNS

Mientras que algunos problemas inherentes a DNS no tienen una fácil solución, hay una serie de medidas que pueden ayudar a minimizar la exposición a algunos de los ataques mencionados.

Una forma de evitar las fugas de información consiste en el uso de una arquitectura comúnmente llamada "split-dns". En ella se separan los servidores DNS internos y externos y se establecen relaciones tales que desde Internet sólo pueden realizarse resoluciones de los sistemas públicamente accesibles. Así mismo, que el DNS utilizado internamente no sea accesible externamente limita la posibilidad de ataques tipo "Cache-snooping", la explotación de vulnerabilidades en el software de servidor DNS o algunos ataques de DNS Spoofing.

Eliminar o limitar la funcionalidad de recursividad, 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. Esto limita la eventualidad de ataques de contaminación de *cache* o vulnerabilidades que necesitan de su presencia para la explotación, o simplemente la posibilidad de que terceros empleen nuestro servidor DNS para sus resoluciones.

Por último, y como ocurre con cualquier software, se deben utilizar siempre las últimas versiones disponibles y aplicar los parches correspondientes para asegurarnos de que no existen vulnerabilidades conocidas en los mismos. ■

Miguel Ángel Hernández Vallejos
Consultor de Seguridad
ESA Security S.A.
mhernandez@esa-security.com

REFERENCIAS

[1] DNS - http://es.wikipedia.org/wiki/DNS
[2] DNSSEC DNS Security Extensions – http://www.dnssec.net
[3] Research Paper - DNS Cache Snooping - http://www.sysvalue.com/papers/DNS-Cache-Snooping/
[4] Welcome To Planet Sony - http://www.doxpara.com/?q=sony
[5] Dsniff - http://monkey.org/~dugsong/dsniff/
[6] DNSA DNS Auditing tool - http://www.packetfactory.net/projects/dnsa/
[7] OzymanDNS 0.1 - http://www.doxpara.com/ozymandns_src_0.1.tgz
[8] Guia rapida de tunneling IP sobre DNS - http://www.digitalsec.es/stuff/texts/dns-tunneling.txt
[9] Bound by Tradition: A Sampling of the Security Posture of the Internet's DNS Servers - http://www.packetfactory.net/papers/DNS-posture/
[10] Lion Worm - http://www.sans.org/y2k/lion.htm
[11] Nameserver DoS Attack October 2002 - http://www.caida.org/projects/dns-analysis/oct02dos.xml