VÍDEO intypedia013es

LECCIÓN 13: SEGURIDAD EN DNS

AUTOR: Javier Osuna García-Malo de Molina

GMV – Jefe de División de Consultoría de Seguridad y Procesos

BERNARDO

Bienvenidos a Intypedia, en esta lección vamos a estudiar, por su importancia, el sistema de nombres de dominio DNS que es ampliamente utilizado en Internet, analizando su utilidad, debilidades y medidas que se pueden adoptar para minimizar ataques. ¡Acompáñanos!

ESCENA 1. EL SISTEMA DNS. CONCEPTOS BÁSICOS

ALICIA

Hola Bernardo, esta mañana la agencia de viajes donde trabaja una amiga ha tenido un problema con su página Web y la forma en la que accedían sus clientes. He mirado su página y parece que un atacante se ha aprovechado del funcionamiento del sistema DNS para simular la página web de la agencia. Su intención era suplantarles y robar información de sus clientes. Como no he estudiado detenidamente cómo funciona internamente DNS, ¿podrías aconsejarme algo para orientar a mi amiga?

BERNARDO

Perfecto Alicia, vayamos por partes. Como sabes, Internet es una red de millones de ordenadores conectados entre sí. Habitualmente, para localizar cada ordenador concreto se utilizan esquemas de direccionamiento. En un mundo analógico, piensa por ejemplo en las direcciones postales que permiten enviar una carta a cada domicilio. En Internet no obstante

es común usar esquemas basados en números; en función de la cantidad y del tamaño de esos números, se puede “acceder” a más o menos ordenadores.

ALICIA

Cierto. En Internet es famoso el esquema de direccionamiento basado en direcciones IP. Por ejemplo, he leído que si el protocolo es IPv4 estas direcciones serán de cuatro números separados por punto; del tipo 172.11.21.108.

BERNARDO

En efecto. Este sistema es muy cómodo para que las máquinas intercambien información, pero a la gente le resulta mucho más sencillo memorizar nombres descriptivos que números de varios dígitos. Si te das cuenta, para llamar a alguien por teléfono, primero buscas su nombre en la agenda. Te resulta mucho más sencillo asociar un nombre o un apodo a una persona que su número de teléfono. Pasa lo mismo con un ordenador o un dispositivo electrónico.

Es precisamente en esto en lo que sistemas de nombre de dominio como el sistema DNS (Domain Name System) tienen utilidad. Al final permite algo tan útil como traducir direcciones “humanas” más o menos descriptivas a direcciones “máquina”, en nuestro caso direcciones IP. Por ejemplo, es más sencillo memorizar o incluso adivinar la dirección correspondiente a la universidad UPM “www.upm.es” que trabajar con su dirección IP, que es “138.100.200.6”. Y no sólo eso, sino que facilita además entre otras funciones el envío de correos electrónicos.

El sistema DNS surge a principios de los 80. Antes de eso, se utilizaba algo más rudimentario: el contenido de un fichero del Sistema Operativo, denominado "**hosts**", para asociar el nombre de dominio con una IP, una especie de agenda local. Hoy día, el sistema DNS es un sistema jerárquico a modo de base de datos distribuida, donde el “elemento inicial” de ese sistema se conoce como servidor raíz. Simplificando un poco este sistema, en general se habla de clientes DNS y servidores DNS. El primero es un software que ejecuta un ordenador para generar peticiones DNS que permitan resolver nombres de dominio, mientras que los servidores DNS intentarán responder a la petición, si no conocen la respuesta a la petición de un cliente podrán reenviar la petición a otro servidor. En Internet puedes profundizar en la arquitectura y comunicación de este sistema, así como en la importancia de los registros DNS para el correcto funcionamiento de la resolución de nombres de dominio de páginas Web, de correo electrónico, etc.

Es importante destacar que debido al hecho de que el número de direcciones IP, el número de peticiones DNS y las exigencias de los usuarios incrementaron notoriamente, el sistema DNS implementó medidas para mejorar el tiempo de respuesta y rendimiento. Para ello los DNS a los que nos conectamos desde nuestra casa o desde la oficina, suelen guardar en una memoria temporal la asociación entre un nombre de dominio, por el que ya han sido consultados, y una o más IPs. El acceso a esta memoria, denominada caché, es mucho más rápido.

ALICIA

Entonces, ¿cada vez que introduzco una url en mi navegador hago una consulta al DNS?

BERNARDO

Siendo estrictos, no toda necesidad de resolución de un dominio tiene que suponer una consulta a un DNS. De hecho, los navegadores Web y los sistemas operativos suelen tener también una caché. Además, es posible introducir la asociación entre un dominio y una IP en el fichero "hosts" tal y como se hacía antes de la existencia de los DNS.

Por ejemplo, en el caso del sistema operativo Windows esto puede realizarse en c:\windows\System32\drivers\etc\hosts.

ALICIA

¡Muy interesante! Además por lo que comentas, parece que este sistema es más crítico de lo que pensaba.

BERNARDO

Así es. Las empresas y organismos públicos son conscientes de la importancia que tiene y del impacto que les puede causar su indisponibilidad. Por este motivo, la seguridad se extrema especialmente en los elementos más importantes del sistema, como pueden ser los servidores raíz que suelen sufrir, por ejemplo, ataques DoS. En cualquier caso vamos analizar algunos de los ataques más famosos a este sistema para que veas la envergadura de lo que hablo y podamos analizar qué le ha sucedido al servidor de tu amiga.

ESCENA 2. ATAQUES AL SISTEMA DNS. MOTIVOS

ALICIA

Vamos al grano Bernardo. ¿Qué me puedes comentar de los ataques más famosos a este sistema y, lo más importante, cuáles son los motivos reales por los que se le ataca?

BERNARDO

Veamos. Hoy día, sin la arquitectura DNS las comunicaciones en Internet se complicarían bastante: acceso a páginas Web, el envío de correos electrónicos, etc. En la práctica, los atacantes se aprovechan de este sistema DNS para suplantar la identidad, espian o robar información. Te voy a resumir algunos de los ataques más típicos, aunque posiblemente en próximas lecciones profundizaremos en cada uno de ellos:

1. Pharming

La mayoría de ataques relacionados con la resolución de dominios tienen por objetivo el robo de credenciales de usuario de bancos, tiendas, redes sociales, juegos online, etc. Para conseguirlo, redireccionan el tráfico dirigido a una Web legítima a otra falsa especialmente preparada para suplantarla; también se puede hacer con el correo electrónico. Si nos centramos en un aspecto local, una de las variantes más comunes del pharming consiste en cambiar el archivo "hosts" del Sistema Operativo atacado. Esto se puede hacer por medio de

un "troyano". Análogamente, sería posible, malintencionadamente claro, tanto modificar en el Sistema Operativo los comandos de consulta a los DNS como cambiar la configuración de conexión a Internet referente a los DNS.

La modificación de los DNS, ya sea la configuración local, los servidores DNS a los que se conectan los usuarios en Internet o mediante un ataque de hombre en el medio, lo habitual es que provoque una redirección de tráfico. Adicionalmente a los problemas de suplantación y robo, debe prestarse atención a este hecho ya que facilitaría la monitorización de las comunicaciones, es decir el espionaje. De hecho, en la actualidad existen propuestas para no depender de la arquitectura DNS tradicional que podría estar controlada por unos pocos países. Soluciones como DNS por p2p, OpenDNS, OpenNIC, etc., cada vez son más mencionados.

2. DNS caché poisoning

En un “envenenamiento de la caché de DNS” el atacante consulta al DNS a comprometer por un dominio que está alojado en un DNS controlado por dicho atacante; a este último lo llamaremos DNS malicioso. Como el DNS a comprometer no tiene cacheado el dominio por el que es preguntado, terminará realizando una consulta al DNS malicioso. El DNS malicioso, además de contestar con la IP asociada al dominio solicitado, contestará con IPs fraudulentas que irán unidas a dominios, por ejemplo, entidades bancarias. El DNS a comprometer responderá a la consulta inicial del atacante con la IP del dominio por el que preguntó y guardará en caché el resto de asociaciones dominio/IP maliciosas.

El DNS comprometido, desde ese momento hasta que los borre de su caché, devolverá las IPs fraudulentas cuando reciba consultas asociadas a los dominios adicionales con los que contestó el DNS malicioso.

En el verano de 2008 el investigador Dan Kaminsky publicó una serie de nuevos descubrimientos que mostraron cómo el problema del envenenamiento era serio y actual, pudiéndose incluso aplicar a escala global en Internet. Por ejemplo, se podría utilizar para comprometer la actualización de aplicaciones, lo que se conoce como evilgrade, de forma que un atacante podría hacerse pasar por el sitio del cual nos descargamos las actualizaciones del sistema operativo.

3. DNS ID Spoofing con Sniffing

DNS ID Spoofing se podría traducir del inglés como "suplantación de identidad en un DNS". Para poder utilizar este ataque se tiene que poder escuchar, o en inglés hacer "sniffing", el tráfico que genera la máquina del usuario a engañar.

En primer lugar, el usuario a engañar lanzará una consulta a un DNS. Esta tiene que tener un identificador entre el 1 y el 65535, que un atacante podrá descubrir escuchando el tráfico. Antes de que el DNS consultado responda, el atacante tendrá que lanzar la respuesta a la petición que la originó, con el mismo identificador que la consulta al puerto, que también ha podido descubrir. Esta respuesta asociará el dominio consultado con una IP fraudulenta. Posteriormente la máquina del usuario a engañar recibirá la respuesta no maliciosa; sin embargo, la desechará al haber ya recibido previamente otra con ese mismo identificador.

Como puedes ver, en la mayoría de los casos el problema viene porque el tráfico DNS, peticiones-respuestas, no están autenticadas lo que simplifica la suplantación-manipulación por parte de un atacante. Este ataque es un ejemplo de ataque de hombre en el medio al protocolo DNS.

ALICIA

Pues sí que hay ataques. ¿Alguno más?

BERNARDO

Vale, este otro es para nota… ¿crees que es posible saber si un DNS ha resuelto un dominio con anterioridad a que le preguntemos por él?

ALICIA

Umm… pues no lo sé.

BERNARDO

La respuesta es afirmativa. A eso se le llama hacer "DNS caché snooping", algo así como fisgonear en la caché del DNS. Por ejemplo, del DNS propio que utilizan los empleados de una empresa se podría obtener información como los bancos con los que trabaja la compañía, los bancos con los que trabajan sus empleados, sus clientes, sus proveedores, los perfiles políticos de sus empleados, software que tienen instalado, etc.

De hecho, en el pasado eran comunes otro tipo de ataques basados en la transferencia de zona, es decir, en aprovechar la mala configuración de un servidor DNS para volcar literalmente los datos de los dominios que gestionaba. En el caso particular del servidor DNS de una organización, este ataque permitía obtener un mapa completo de la red interna de una organización: hosts, direcciones IP internas, etc.

ALICIA

Pero eso parece no ser tan grave…

BERNARDO

De acuerdo, es menos peligroso que otros ataques pero piensa que, además de tener implicaciones legales, esa información se podría usar entre otras cosas para, a su vez, realizar ataques como phishing, ingeniería social o la explotación eficiente de vulnerabilidades software.

Además existen otros usos aprovechándose de la arquitectura DNS pero ya tendremos tiempo en el futuro de hablar de esteganografía con DNS, distribución de malware vía DNS, fast flux, etc.

ESCENA 3. RECOMENDACIONES Y SECURIZACIÓN.

ALICIA

Bernardo, ¿entonces qué se puede hacer para minimizar ataques de este tipo? Algo le tendré que decir a mi amiga…

BERNARDO

Por un lado están las medidas tradicionales. Desde un punto de vista del usuario, hay que tomar las medidas oportunas para que tu ordenador y router estén debidamente protegidos: como ya hemos comentado en anteriores lecciones, actualizar el software, configurar adecuadamente un antivirus, usar cortafuegos, una política de claves correcta, etc. En la mayoría de las ocasiones los ataques serán por esta vía. Por otro lado, si tu misión es proteger una infraestructura, entonces deberías disponer de un control de accesos sólido, disponer de un sistema de monitorización efectivo, concienciar a los empleados frente a técnicas de ingeniería social, que sólo se pueda acceder a la caché del DNS desde máquinas alojadas en la red interna, tener implantadas las versiones actualizadas de software en los DNS, configurar los servicios correctamente, etc. Además, si en el peor de los casos sufres un ataque, es fundamental disponer de trazas de los DNS de quién, qué y cuándo se realizan cambios en la información de los DNS para ser capaz de detectar qué ocurrió y cómo.

Sin duda el mayor problema del DNS es que en su diseño no se consideraron aspectos de seguridad. Hoy día existen estándares, como el DNSSEC (Domain Name System Security Extensions) del IETF (Internet Engineering Task Force), que proporciona autenticación e integridad de los datos intercambiados vía DNS, usando criptografía de clave pública, lo que dificulta ataques de suplantación. Así que hay que estar atentos a estas propuestas para mejorar la seguridad global.

ALICIA

Me has aclarado muchas cosas Bernardo, gracias. Creo que con esta información ya podré orientar a mi amiga para que aconseje a sus clientes la forma más segura de conectarse a su agencia. Creo que por hoy es suficiente. En la Web de Intypedia encontrarás información adicional a esta lección, especialmente de la arquitectura del sistema DNS. ¡Hasta luego!

BERNARDO

¡Hasta pronto!

Guión adaptado al formato Intypedia a partir del documento entregado por D. Javier Osuna García-Malo de Molina

Madrid, España, febrero de 2012

http://www.intypedia.com

http://twitter.com/intypedia