**¿Qué es un servidor DNS?**

Un servidor DNS es un servidor que se encarga de almacenar en sus registros las IPs asociadas a los distintos dominios que hay en la web. Es decir, cuando una computadora teclea un nombre de dominio, debe saber cuál es la IP asociada a ese nombre de dominio, y una de las formas más fáciles de lograr saberlo es realizarle una consulta a uno de estos servidores que se encargan de almacenar en grandes cantidades estos directorios.

Un ordenador normal tiene un caché de DNS en el que almacena direcciones para no tener que pedirlas constantemente al servidor, pero su almacenamiento no es de un tamaño comparable al de un servidor.

**¿Cómo puede el servidor DNS sufrir ataques?**

Existen tres tipos de ataques DNS posibles:

Envenamiento de caché DNS: Como dijimos, tanto el servidor como la máquina del usuario guardan direcciones DNS en su caché. Un hacker puede entrar a una máquina usuario y modificar el documento donde se guardan estos DNSs e implantar las direcciones de sus sitios maliciosos, haciendo que la máquina se dirija a ellos cuando el usuario ingresa la dirección de un sitio legítimo.

De la misma manera, esto le puede suceder al servidor. Si el servidor tiene almacenadas direcciones y un atacante logra acceder, puede lograr modificar las direcciones de ese servidor. Hay servidores que tienen consultas recursivas y no recursivas. Recursivas significa que el servidor, cada cierto tiempo o ciclos, vuelve a enviar una consulta a otros servidores para renovar su lista de DNSs guardados. Entonces, si es un servidor no recursivo, guardará todas las direcciones permanentemente, y ahí es donde el atacante puede modificarlas.

Ataque DOS: Como cualquier servidor, los servidores DNS son vulnerables a un ataque DOS donde el servidor es sobrecargado por demasiados pedidos y cae. Esto puede ser una táctica útil porque así un atacante puede tirar un servidor legítimo con direcciones DNS verdaderas, y en su lugar implantar un servidor malicioso que redirige a las páginas que el atacante quiere. Esto a su vez sirve también para envenenar servidores de consultas recursivas, puesto que cuando estos servidores quieran saber la dirección de un sitio y deban buscarla mediante otros servidores, irán al servidor malicioso sin saberlo.

El servicio DHCP o Dynamic Host Control Protocol, por su nombre en inglés, es un protocolo de autoasignación de IPs a los ordenadores en una red. Al ser automático, facilita la configuración de nuevos dispositivos que se añadan a la red al no tener que manualmente configurar cada uno de ellos, lo cual tomaría demasiado tiempo considerando la cantidad de dispositivos IoT hoy en día.

Existen dos tipos de ataques principales contra el DHCP:

El primero es un ataque de DHCP starving, que consiste en enviar muchas peticiones DHCP desde dispositivos falsos, para lograr que el DHCP se quede sin direcciones IP disponibles y no pueda asignarlas a nuevos usuarios.

Esto se puede considerar un ataque DOS, ya que estamos literalmente negando el servicio a otros. Además, al intentar procesar tantos pedidos, puede que el servidor simplemente se caiga.

DHCP Spoofin: Un ataque Man in the Middle donde montamos nuestro propio servidor DHCP malicioso y hacemos que la gente reciba sus direcciones IP desde nuestro servidor en vez del legítimo. Así, todo el tráfico pasa por nosotros y podemos leerlo. Esto se suele hacer en combinación con el ataque DOS al servidor original.

Se puede prescindir tanto de un servidor DNS como de un protocolo DHCP. Sin embargo, el trabajo que ello supondría es inmenso:

Prescindir del servidor DNS implica que nuestra máquina debería guardar todas las direcciones IP que necesite, y esto conllevará una gran cantidad de espacio. Si llegásemos a no guardarlas, deberíamos usar una página o base de datos para ver todas las direcciones DNS que necesitemos en un momento determinado.

Por otro lado, con respecto al servidor DHCP, podríamos prescindir de él y simplemente configurar manualmente cada dispositivo que se conecta a una red. Esto no es tan engorroso en una red pequeña, pero se volvería rápidamente un problema de gestionar en una red grande, o con muchos dispositivos IoT o con un cambio grande de dispositivos.