Ataque de denegación de servicio

En seguridad informática, un **ataque de denegación de servicio**, también llamado **ataque DoS** (de las siglas en inglés *Denial of Service*), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

Se genera mediante la saturación de los puertos con flujo de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando servicios, por eso se le dice "denegación", pues hace que el servidor no dé abasto a la cantidad de usuarios. Esta técnica es usada por los llamados crackers para dejar fuera de servicio a servidores objetivo.

El llamado **DDoS** (siglas en inglés de *Distributed Denial of Service*, denegación de servicio distribuida) es una ampliación del ataque DoS, se efectúa con la instalación de varios agentes remotos en muchas computadoras que pueden estar localizadas en diferentes puntos. El invasor consigue coordinar esos agentes para así, de forma masiva, amplificar el volumen de saturación de información, pudiendo darse casos de un ataque de cientos o millares de computadoras dirigido a una máquina o red objetivo. Esta técnica se ha revelado como una de las más eficaces y sencillas a la hora de colapsar servidores, la tecnología distribuida ha ido sofisticándose hasta el punto de otorgar poder de causar daños serios a los ordenadores de personas con escaso conocimiento técnico.

En ocasiones, esta herramienta ha sido utilizada como un notable método para comprobar la capacidad de tráfico que un ordenador puede soportar sin volverse inestable y perjudicar los servicios que desempeña. Un administrador de redes puede así conocer la capacidad real de cada máquina.

Un ejemplo actual: el viernes 20 de febrero de 2009, se produjo un gran ataque DDoS contra un servidor de DhapCenter S.L. (Paterna - Valencia), el ataque provino desde cientos de lugares distintos y provocó la caida de una red de 400 Mbits (casi 4gbps) y la caida de todo el centro de datos de Dhapcenter y Abansys, una de las webs alojadas es sardá.es</ref>

Métodos de ataque

Un ataque de "Denegación de servicio" impide el uso legítimo de los usuarios al usar un servicio de red. El ataque se puede dar de muchas formas. Pero todas tienen algo en común: utilizan el protocolo TCP/IP para conseguir su propósito.

Un ataque DoS puede ser perpetrado in un numero de formas. Aunque basicamente consisten en :

1. Consumo de recursos computacionales, tales como ancho de banda, espacio de disco, o tiempo de procesador.
2. Alteración de informacion de configuración, tales como información de rutas de encaminamiento.
3. Alteración de información de estado, tales como interrupción de sessiones TCP (TCP reset).
4. Interrupción de componentes físicos de red.

5. Obstrucción de medios de comunicación entre usuarios de un servicio y la victima, de manera que ya no puedan comunicarse adecuadamente.

Inundación SYN (SYN Flood)

Principios de TCP/IP

Cuando una máquina se comunica mediante TCP/IP con otra, envía una serie de datos junto a la petición real. Estos datos forman la cabecera de la solicitud. Dentro de la cabecera se encuentran unas señalizaciones llamadas Flags (banderas). Éstas señalizaciones (banderas) permiten iniciar una conexión, cerrarla, indicar que una solicitud es urgente, reiniciar una conexión, etc. Las banderas se incluyen tanto en la solicitud (cliente), como en la respuesta (servidor).

Para aclararlo, veamos cómo es un intercambio estándar TCP/IP:

- 1 Establecer Conexión: El cliente envía una Flags SYN, si el servidor acepta la conexión este debería responderle con un SYN/ACK luego el cliente debería responder con una Flags ACK.

```
1-Cliente --------SYN-----> 2 Servidor 4-Cliente <-----SYN/ACK---- 3 Servidor
5-Cliente --------ACK-----> 6 Servidor
```

- 2 Resetear Conexión: Al haber algún error o perdida de paquetes de envio se establece envio de Flags RST:

```
1-Cliente   -------Reset----->   2-servidor   4-Cliente   <----Reset/ACK----
3-Servidor 5-Cliente --------ACK------- 6-Servidor
```

La inundación SYN envía un flujo de paquetes TCP/SYN (varias peticiones con Flags SYN en la cabecera), muchas veces con la dirección de origen falsificada. Cada uno de los paquetes recibidos es tratado por el destino como una petición de conexión, causando que el servidor intente establecer una conexión al responder con un paquete TCP/SYN-ACK y esperando el paquete de respuesta TCP/ACK (Parte del proceso de establecimiento de conexión TCP de 3 vías). Sin embargo, debido a que la dirección de origen es falsa o la dirección IP real no ha solicitado la conexión, nunca llega la respuesta.

Estos intentos de conexión consumen recursos en el servidor y limitan el número de conexiones que se pueden hacer, reduciendo la disponibilidad del servidor para responder peticiones legítimas de conexión.

Ataque LAND (LAND attack)

Un ataque LAND se realiza al enviar un paquete TCP/SYN falsificado con la dirección IP del servidor objetivo como si fuera la dirección origen y la dirección destino a la vez, además de usar un puerto abierto TCP, tanto de destino como de origen. Esto causa que el servidor se responda a sí mismo continuamente hasta colapsar sus recursos.

Cómo evitar el ataque LAND La mayoría de los Firewalls deberian interceptar el paquete malicioso. Adicionalmente, routers deberín ser configurados con filtros tanto de entrada como de salida, para bloquear tráfico donde la dirección IP origen se encuentra en el mismo espacio de direcciones que la dirección destino. Algunos sistemas operativos han generado actualizaciones para específicamente cubrir este problema de seguridad.

Inundación ICMP (ICMP Flood)

Es una técnica DoS que pretende agotar el ancho de banda de la víctima. Consiste en enviar de forma continuada un número elevado de paquetes ICMP Echo request (ping) de tamaño considerable a la víctima, de forma que esta ha de responder con paquetes ICMP Echo reply (pong) lo que supone una sobrecarga tanto en la red como en el sistema de la víctima.

Dependiendo de la relación entre capacidad de procesamiento de la víctima y atacante, el grado de sobrecarga varía, es decir, si un atacante tiene una capacidad mucho mayor, la víctima no puede manejar el tráfico generado.

SMURF

Existe una variante a *ICMP Flood* denominado Ataque Smurf que amplifica considerablemente los efectos de un ataque ICMP.

Existen tres partes en un Ataque Smurf: El atacante, el intermediario y la víctima (comprobaremos que el intermediario también puede ser víctima).

En el ataque Smurf, el atacante dirige paquetes ICMP tipo "*echo request*" (ping) a una dirección IP de broadcast, usando como dirección IP origen, la dirección de la víctima (Spoofing). Se espera que los equipos conectados respondan a la petición, usando *Echo reply*, a la máquina origen (víctima).

Se dice que el efecto es amplificado, debido a que la cantidad de respuestas obtenidas, corresponde a la cantidad de equipos en la red que puedan responder. Todas estas respuestas son dirigidas a la víctima intentando colapsar sus recursos de red.

Como se dijo anteriormente, los intermediarios también sufren los mismos problemas que las propias víctimas.

Inundación UDP (UDP Flood)

Básicamente este ataque consiste en generar grandes cantidades de paquetes UDP contra la víctima elegida. Debido a la naturaleza sin conexión del protocolo UDP, este tipo de ataques suele venir acompañado de IP Spoofing.

Es usual dirigir este ataque contra máquinas que ejecutan el servicio Echo, de forma que se generan mensajes Echo de un elevado tamaño.

Véase también

- Ping de la muerte
- DDoS
- Nuke
- Flags
- Ataque Smurf

Referencias externas

Enlaces externos

- Intentando detener un DDoS [1]
- Comunicado de prensa de un comercio online que sufrió ataques DDoS [2]

Referencias

[1] http://foro.elhacker.net/index.php/topic,137442.0.html
[2] http://dvdbarato.net/correos/0809_1

Fuentes y contribuyentes del artículo

Ataque de denegación de servicio *Fuente*: http://es.wikipedia.org/windex.php?oldid=27273403 *Contribuyentes*: AlexGPL, Alexisabarca, Aloriel, Antojio, Antur, Cinabrium, DMG, Daniel G., Dav7mx, Dodo, Emijrp, GermanX, Ghostbar, Huds, Jjvaca, Jugones55, Kekkyojin, Leandrosw, Manuelt15, Montgomery, Mortadelo, Nelsito777, Orgullomoore, Paintman, RICARDOSA, Rizome, Rllaque, Superzerocool, X.Cyclop, 77 ediciones anónimas

Licencia