Ataques DOS

Los ataques DOS (denegación de servicio) causan todos los años pérdidas millonarias a empresas, y muchos problemas a los administradores de sistemas. Y es que no hace falta mucho para llevarlos a cabo.
Esta facilidad de uso hace que muchos, sin tener los conocimientos necesarios sobre un protocolo, sigan cualquier tutorial que se encuentren en internet y lleguen a causar grandes daños.

Connection Flood

las emptesas de IT que utilisen servidores tienen un numero maximo de conexiones que pueda tener su servicion en un momento dado. Una vez que se alcanza ese límite, no se admitirán conexiones nuevas. Por ejemplo: si un servidor Web tiene capacidad para mil usuarios conectados y un atacante establece mil conexiones pero sin realizar ninguna petición el monopolizará dicho servidor. Las conexiones van caducando por inactividad poco a poco, pero el atacante sólo necesita intentar nuevas conexiones, para mantener fuera de servicio el servidor.

ICMP Flood

Este ataque consiste en saturar el recurso de destino con solicitudes de paquetes “eco” ICMP (ping), básicamente se trata de enviar paquetes de solicitud sin esperar los paquetes de respuesta. Este tipo de ataque consume ancho de banda tanto saliente como entrante, hasta lograr la caída del servicio o el reinicio de la máquina. Los ataques mediante ICMP flood pueden ser detenidos gracias a la configuración de Listas de Control de Acceso (ACL’s) en routers y switches.

Net Flood

En estos casos, la red víctima no puede hacer nada. Aunque filtre el tráfico en sus sistemas, sus líneas estarán saturadas con tráfico malicioso, incapacitándolas para cursar tráfico útil.
Un ejemplo habitual es el de un teléfono: si alguien quiere molestar, sólo tiene que llamar, de forma continua.
En el caso del Net Flooding el atacante envía tantos paquetes de solicitud de conexión que las conexiones auténticas simplemente no pueden competir. Como cuando alguien intenta mandar un fax empleando el número de voz: el fax insiste durante horas, sin que el usuario llamado pueda hacer nada al respecto.
En casos así el primer paso a realizar es el ponerse en contacto con el Proveedor del servicio para que intente determinar la fuente del ataque y, como medida provisional, filtre el ataque en su extremo de la línea.
El siguiente paso consiste en localizar las fuentes del ataque e informar a sus administradores, ya que seguramente se estarán usando sus recursos sin su conocimiento y consentimiento.

Smurf

En un ataque “pitufo”, los atacantes usan la suplantación de su dirección IP para que sea la misma que la dirección IP de la víctima. Esto causará una gran confusión en la red de la víctima, y se enviará una avalancha masiva de tráfico al dispositivo de red de la víctima, si se realiza correctamente. La mayoría de los firewalls protegen contra los ataques de los pitufos, pero hay varias cosas que uno puede hacer. Si tiene acceso al enrutador en el que se encuentra su red o sitio web, simplemente configurelo para que no reenvíe paquetes a las direcciones de difusión.

UDP Flood

Este ataque DDoS aprovecha el protocolo UDP (User Datagram Protocol), un protocolo de red que no necesita una sesión iniciada en el equipo remoto. Este tipo de ataque inunda puertos aleatorios de dicho host remoto con numerosos paquetes UDP , causando que el equipo víctima compruebe ante cada petición a cada puerto, si hay alguna aplicación escuchando en destino; y en caso de no haberla responde con un paquete ICMP (Internet Control Message Protocol) de error de destino. Al ser el número de paquetes enviado enormemente exagerado, este proceso agota los recursos del servidor o equipo, y en última instancia puede conducir a la inaccesibilidad.

Snork UDP

Este ataque es dirigido contra sistemas Windows. En este caso se emplea un paquete de datos UDP con origen en el puerto 7 (servicio “echo”) o el puerto 19 (servicio “chargen”), utilizando como puerto de destino el 135, en el que se ubica el servicio de localización de Microsoft a través del protocolo NetBIOS. De este modo, se consigue un intercambio de paquetes UDP innecesario que reduce el rendimiento de los equipos y de la red afectada. Se trata, por tanto, de otro ataque del tipo “reflector attack”.

Fuentes:
https://openwebinars.net/blog/top-10-de-ataques-dos-denial-of-service-o-denegacion-de-servicios/
http://www.ids-sax2.com/articles/PreventDosAttacks.htm
https://www.edisa.com/wp-content/uploads/2014/08/Ponencia_-_Tipos_de_ataques_y_de_intrusos_en_las_redes_informaticas.pdf
https://www.segu-info.com.ar/ataques/ataques_dos.htm