**Denegación de servicio**

* **Descripción de la amenaza.**

La denegación de servicio es un ataque con el propósito de interrumpir el correcto funcionamiento de una máquina o red, dejándola inaccesible para los usuarios. Los atacantes consiguen el objetivo mediante la inundación del objetivo con tráfico de red, o enviando información que provoca la caída del servicio.

Las víctimas habituales de ataques DoS son servidores web de organizaciones importantes como las bancarias, de comercio, medios de comunicación y gubernamentales. Aunque los ataques DoS normalmente no resultan en el robo o la pérdida de información importante u otros recursos, sí que pueden costar a la víctima una gran cantidad de dinero y tiempo para solucionar el problema.

Hay 2 métodos generales de realizar un ataque DoS: inunda servicios o provocar un “crash” del servicio. Los ataques de inundación ocurren cuando el sistema recibe demasiado tráfico, causando que se ralentice e incluso deje de funcionar al completo.

Los ataques de inundación populares son:

* **Ataques de buffer overflow**: es el ataque DoS más común. El concepto consiste en enviar más tráfico a una dirección de red del que los programadores del sistema establecieron en su momento como tráfico previsto. Incluye los otros tipos de ataque, además de otros que están diseñados para abusar bugs específicos de ciertas aplicaciones o redes.
* **Inundación ICMP**: se aprovecha de los dispositivos de red mal configurados mediante el envío de paquetes falsificados que realizan un ping a cada sistema de la red de destino, en lugar de solo a una máquina específica. Esto provoca que la red se active para amplificar el tráfico. Este tipo también se conoce como ataque smurf o ping de la muerte.
* **Inundación SYN**: envía una petición para conectarse a un servidor, pero nunca completa el *handshake.* Continúa hasta que todos los puertos están saturados con peticiones y ninguno está disponible para que se conecten a él los usuarios legítimos.
* **Riesgos que supone.**
* **Falta de disponibilidad**: los usuarios legítimos podrían no tener acceso a los recursos a los que esperan acceder y no serán capaces de encontrar la información que necesitan o llevar a cabo las acciones que requerían.
* **Pérdidas económicas**: la organización afectada podría no ser capaz de continuar con alguna de sus actividades críticas, sobre todo aquellas que requieren ser ejecutadas rápidamente. Por otra parte, para solucionar el problema, los empleados de TI de la empresa podrían ser necesitados durante un tiempo extra al habitual, resultando en más costes.
* **Reputación afectada**: cuando ocurre un incidente de este tipo, la imagen de la empresa se ve afectada negativamente y esto puede afectar a la relación con los clientes.
* **Pérdida de clientes**: los clientes, al conocer la existencia de un ataque de este tipo, podrían optar por escoger a un competidor de la empresa afectada para llevar a cabo los servicios que requieren de ahora en adelante.
* **Medidas correctivas.**
* **Adquisición de un nuevo producto:** adquisición de software y hardware de monitorización y análisis de tráfico de red. Se debería supervisar el tráfico mediante sistemas IDS (Intrusion Detection System). Los administradores de red deben establecer reglas para crear alertas para tráfico inusual, identificar las fuentes del tráfico y descartar paquetes de red que encajen con un criterio decidido.
* **Contratación de un nuevo servicio:** contratar servicio cloud para los sistemas más críticos. El cloud generalmente proporciona más ancho de banda que los recursos on-premise y la naturaleza del cloud significa que muchos servidores no estarán situados en el mismo espacio físico, de esta manera es más difícil para el atacante interrumpir el correcto funcionamiento de los sistemas de información de la organización.
* **Ejecución de un cambio interno:** establecer un plan de respuesta ante un ataque DoS. Debe incluir aspectos de comunicación, mitigación y recuperación. Se debe practicar de manera simulada en lugar de esperar a que ocurra un ataque real.
* **Ejemplos de ataques DoS (casos reales).**

Los casos presentados a continuación son algunos de los ejemplos más famosos de **Distributed** Denial of Service, es decir, ataques DoS realizados por múltiples fuentes coordinadas.

* **El ataque DDoS a AWS en 2020**: Amazon Web services fue víctima de un gigantesco ataque DDoS en febrero de 2020. Fue uno de los ataques DDoS recientes más extremos de la historia y se dirigió a un cliente de AWS no identificado mediante una técnica llamada Protocolo ligero de acceso a directorios sin conexión (CLDAP). El ataque duró **3 días** y su pico de tráfico enviado alcanzó los **2.3 terabytes por segundo**.
* **El ataque a Google en 2020**: el 16 de octubre de 2020, el TAG (Threat Analysis Group) de Google, publicó una actualización referente a cómo las amenazas y los actores de estas estaban cambiando debido a las elecciones de EE.UU de 2020.

Según la explicación que dan, los ingenieros detectaron un ataque de amplificación UDP récord proveniente de una gran cantidad de ISPs chinos (ASNs 4134, 4837, 58453, y 9394), resultando en el ataque de mayor ancho de banda jamás registrado.

El pico de tráfico fue 2.5Tbps. El atacante utilizo múltiples redes para falsificar 167 millones de paquetes por segundo hacia 180.000 servidores de tipo CLDAP, DNS y SMTP.

* **Ataque a GitHub en 2018**: el 28 de febrero de 2018, GitHub fue víctima de un ataque DDoS que alcanzó los 1.35 terabits por segundo y duró alrededor de 20 minutos constantes. Según los portavoces de GitHub, el ataque se asoció a más de 1.000 sistemas autónomos (ASNs) diferentes distribuidos en decenas de miles de endpoints únicos.
* **Ataques Mirai Kbres y OVH en 2016**: el 20 de setiembre de 2016, el blog del experto en ciberseguridad Brian Krebs fue asaltado por un ataque DDoS en exceso de 620 Gbps. Aunque su blog había sido atacado en 269 ocasiones por ataques DDoS desde 2012, este fue el triple de grande que cualquier otro previo.

La fuente consistía en la botnet Mirai, que a finales de ese mismo año consistía ya de más de 600.000 dispositivos IoT comprometidos como cámaras IP, routers domésticos, etc.

Por otra parte, la botnet Mirai atacó también el 19 de setiembre a uno de los proveedores de hosting europeos más importantes: OVH. Se realizó sobre uno de los clientes de OVH y los responsables eran aproximadamente 145.000 bots, generando una carga de tráfico de hasta 1.1 terabits por segundo y duró 1 semana.