# Ataque DoS

El ataque de Denegación de Servicio (DoS) es un ciberataque en el que el ciberdelincuente tiene como objetivo que un ordenador o servicio no esté disponible para los usuarios a los que va dirigidos, interrumpiendo el funcionamiento normal del mismo. Estos ataques suelen funcionar al sobrecargar o inundar una maquina objetivo con solicitudes hasta que sea incapaz de procesar el tráfico normal. Se caracteriza por utilizar un único ordenador para lanzar dicho ataque.

# ¿Cómo funciona?

## Ataque de desbordamiento de búfer

Este tipo de ataque se aprovecha de vulnerabilidades en la gestión de la memoria por parte del software. Al enviar más datos de los que un búfer de memoria puede contener, se produce un desbordamiento que puede corromper la memoria, provocar fallos en el sistema e incluso permitir la ejecución de código malicioso.

## Ataque de inundación

Consiste en inundar el servidor objetivo con un volumen abrumador de tráfico, superando su capacidad de procesamiento. Existen diferentes tipos de ataques de inundación, como:

- **Inundación SYN (SYN Flood)**: Se envían múltiples peticiones de conexión SYN a un servidor, pero no se completa el handshake TCP (no se envía el paquete ACK de confirmación). Esto satura la cola de conexiones pendientes del servidor, impidiendo que procese nuevas conexiones legítimas.
- **Inundación UDP (UDP Flood)**: Se envían paquetes UDP masivos al servidor objetivo. A diferencia de TCP, UDP es un protocolo sin conexión, por lo que el servidor intenta procesar cada paquete UDP que recibe. Un volumen masivo de paquetes UDP puede saturar el servidor y consumir su ancho de banda.