DoS Attack

Denial of Service (DoS) attack is a cyber attack in which a cybercriminal aims to make a computer or service unavailable to targeted users, disrupting the normal operation of the computer or service. These attacks typically work by overloading or flooding a target machine with requests until it is unable to process normal traffic. It is characterized by using a single computer to launch the attack.

How does it work?

Buffer overflow attack

This type of attack takes advantage of vulnerabilities in the software's memory management. By sending more data than a memory buffer can hold, an overflow occurs that can corrupt memory, cause system crashes, and even allow malicious code to be executed.

Flood attack

This consists of flooding the target server with an overwhelming volume of traffic, exceeding its processing capacity. There are different types of flood attacks, such as:

- SYN Flood: Multiple SYN connection requests are sent to a server, but the TCP handshake is not completed (the confirmation ACK packet is not sent). This saturates the server's queue of pending connections, preventing it from processing new legitimate connections.
- UDP Flood: Massive UDP packets are sent to the target server. Unlike TCP, UDP is a connectionless protocol, so the server tries to process every UDP packet it receives. A massive volume of UDP packets can saturate the server and consume its bandwidth.