What is it?

Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks are mainly known for their ability of denying the access to several computer resources or reducing the performance of a specific service or connectivity by overloading the network or system resources such as network bandwidth, router processing capability etc.

The DoS attacks can occur in two methods:

1. The attacker causes the servers to crash or degrade their performance by exploiting the existing software flaws
2. The attacker sends a large number of fraudulent request until the victim’s CPU, memory or network resources are overwhelmed

The Distributed-Denial-of-Service (DDoS) are a more updated version of the Denial-of-Service attacks. It uses slave machines to which it distributes the responsibilities and as a result increase the threat. The impact of multiple attackers is not only greater but also much more difficult to detect.

The DoS attacks can be classified as follows based on the number of attackers and the volume of packets:

1. Software exploits: can easily disable its target with a single or few packets by using specific software bugs. The only way this type of DoS attack can be prevented is by always making sure to be on top of the latest software update.
2. Flooding attacks: based on the number of attackers, they can be further split into single-source and multi-sources attacks. This type of attack operates by sending endless streams of packets until all resources are overwhelmed.

There are two main categories in which we can split the DDoS attacks:

1. Bandwidth Depletion: the victims network is being flooded with unsolicited requests so that the legitimate ones are prevented from reaching the system.
2. Resource Depletion: targets a process or a server on the system making it unable to process requests by tying up its resources. It either utilizes vulnerable portions of a protocol or sends incorrectly formed IP packets in order to crash the system.

**How to detect it**

It is almost impossible to detect such attacks. However, the ones generated by available tools have identifying characteristics making the detection possible in some cases.

Detection mechanisms such as entropy based detection, statistical and UNN based detection has been proposed.

**Prevention measures**

Upgrading faulty software or filtering particular packet sequences are the most efficient methods when it comes to preventing these attacks.

Often spoofed source IP addresses are used in order for the attacker not to be traced back, hence another prevention measure could be preventing IP spoofing first.