**Teardrop attack**

**Description 1**

A teardrop attack is a denial-of-service (DoS) attack that involves sending fragmented packets to a target machine. Since the machine receiving such packets cannot reassemble them due to a bug in TCP/IP fragmentation reassembly, the packets overlap one another, crashing the target network device. This generally happens on older operating systems such as Windows 3.1x, Windows 95, Windows NT and versions of the Linux kernel prior to 2.1.63.

One of the fields in an IP header is the “fragment offset” field, indicating the starting position, or offset, of the data contained in a fragmented packet relative to the data in the original packet. If the sum of the offset and size of one fragmented packet differs from that of the next fragmented packet, the packets overlap. When this happens, a server vulnerable to teardrop attacks is unable to reassemble the packets - resulting in a denial-of-service condition. [1]

**Description 2**

A DoS attack where fragmented packets are forged to overlap each other when the receiving host tries to reassemble them. [2]

**Description 3**

In this type of attack first a packet of small size is sent. Then another packet said to be the part of the first packet sent. The second packet sent is very small to pick it from the first packet, this causes an error is assembling and the system may crash or hang. Generally fragmentation is very necessary if the message size is large , at the receiving end all the fragmented packets are reassembled to complete it, teardrop attacks concentrate here and sends unrelated fragment packets, which leads to system crash or hang when trying to assemble them. [3]

**Reference**

[1] <https://security.radware.com/ddos-knowledge-center/ddospedia/teardrop-attack/>

[2] <http://www.webopedia.com/TERM/T/Teardrop_attack.html>

[3] <https://www.hostdepartment.com/blog/2014/05/21/ddos-attack/>