**UDP Flood**

**Description 1**

UDP flooding is similar to ping flood. Here instead of ping packets, UDP packets are bombarded against the server. UDP could be a lot more effective than ICMP in smaller networks as the size of the UDP packets are enormous. The packet size could be set up to 65000 bytes which could easily flood a given Ethernet network when multiple zombies are set up. This project has analyzed all the above described attacks and has brought down some interesting observations. [1]

**Description 2**

A UDP flood is a network flood and still one of the most common floods today. The attacker sends UDP packets, typically large ones, to single destination or to random ports. In most cases the attackers spoof the SRC IP which is easy to do since the UDP protocol is “connectionless” and does not have any type of handshake mechanism or session.

The main intention of a UDP flood is to saturate the Internet pipe. Another impact of this attack is on the network and security elements on the way to the target server, and most typically the firewalls. Firewalls open a state for each UDP packet and will be overwhelmed by the UDP flood connections very fast. [2]

**Reference**

[1] [**https://www.sans.org/reading-room/whitepapers/detection/denial-service-attacks-mitigation-techniques-real-time-implementation-detailed-analysi-33764**](https://www.sans.org/reading-room/whitepapers/detection/denial-service-attacks-mitigation-techniques-real-time-implementation-detailed-analysi-33764)

[2] <https://security.radware.com/ddos-knowledge-center/ddospedia/udp-flood/>