**TCP SYN Flood**

**Description 1**

Flooding attacks (like Smurf and ping flood attacks) consuming the bandwidth space whereas this attack aims at exploiting server CPU memory. Whenever a host attempts to connect to a server, a three-way handshake protocol is established before any actual data transfer occurs. Firstly, the host sends a SYN packet to initiate the handshake. The server then replies with an Acknowledgement packet. At last the host again needs to send a SYN ACK packet to establish a successful connection. But attackers leave the handshake half open by not sending the last SYN and the server keeps waiting for the host to send the final packet. When thousands of such half open connections are initiated, the server runs out of memory and crashes. It will not be able to serve the legitimate clients as its memory is dumped with forged fake packets. [1]

**Description 2**

A SYN flood is a type of Denial of Service attack. We can say that a victim host is under a SYN flooding attack when an attacker tries to create a huge amount of connections in the SYN RECEIVED state until the backlog queue has overflowed. The SYN RECEIVED state is created when the victim host receives a connection request (a packet with SYN flag set) and allocates for it some memory resources. A SYN flood attack creates so many half-open connections that the system becomes overwhelmed and cannot handle incoming requests any more. [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://www.symantec.com/connect/articles/hardening-tcpip-stack-syn-attacks>