SYN Flood

SYN Flood

SYN Flood attack is a type of Denial of Service attack that exploits the normal three-way handshake to consume resources on the targeted server and render it unresponsive.

In SYN Flood attack, the attacker floods every port on target server by sending repeated SYN packets. Attacker fills the server's network connection table with half open connections. Resulting an unfinished TCP 3-way handshake. Several SYN request packets are flooded to a victim machine which results a victim's machine to slow down or crash and shutdown lead to denial of service (DOS).

Attacks

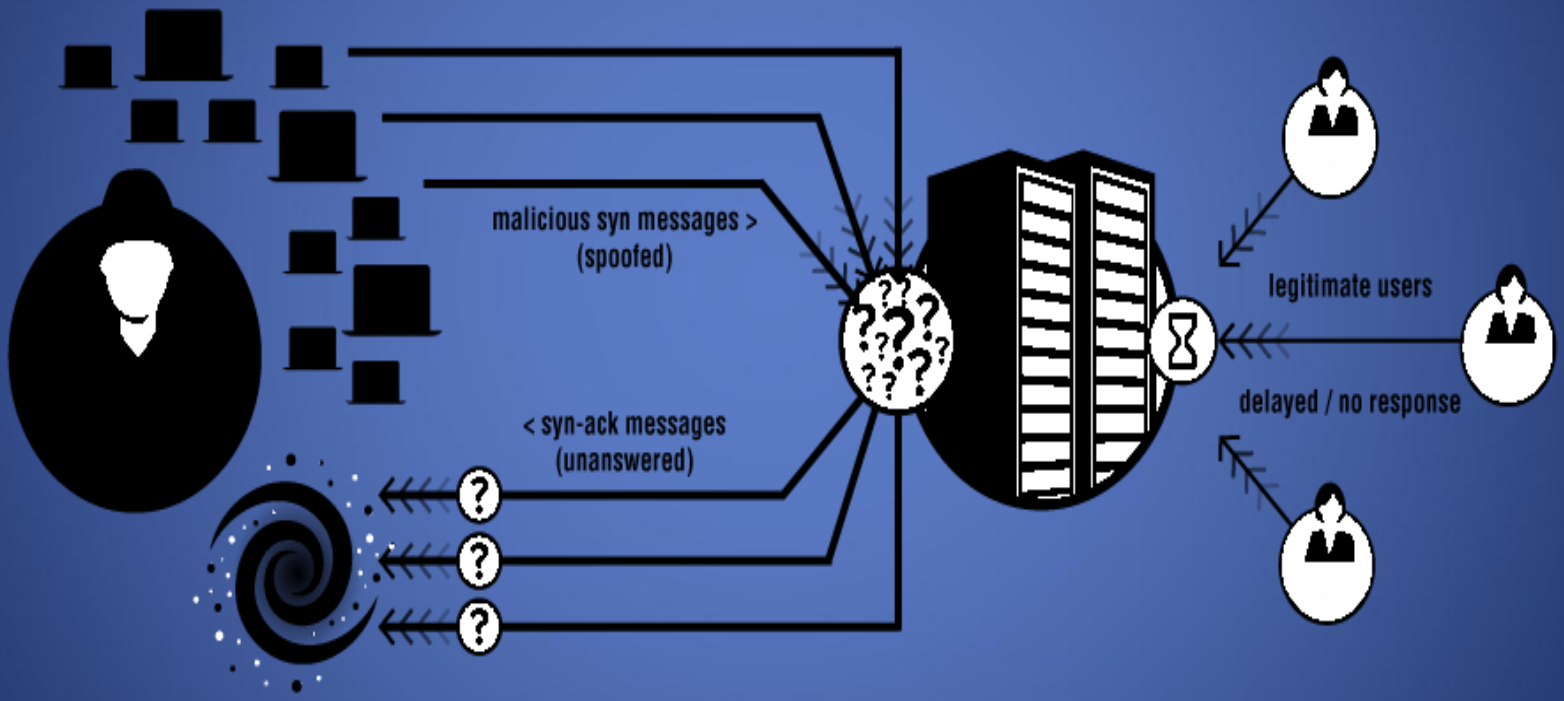
Denial-of-service attacks: DoS attacks often leverage SYN Flood to link multiple IP addresses with a victim machine IP address. As a result, a victim machine will flooded with SYN request from multiple spoofed IP address over the network. Resulting the victim machine to crash.

Example

In a TCP/IP client server communication a client initiates a TCP request with SYN (Synchronize) message, Where the server respond back with SYN-ACK (acknowledgement) message to client SYN request with its own SYN message. After receiving the SYN-ACK message from server, client Acknowledge back with ACK message and the TCP session is established between client and server.

An attacker send a SYN request from several fake IP address to initiate a TCP session request. The victim machine response back with the SYN-ACK message to those fake SYN request which never get resolved, as a result the victim machine resource is overloaded with half open face SYN request leading to DOS.

Example


malicious syn messages >
(spoofed)
< syn-ack messages
(unanswered)
legitimate users
delayed / no response