

TCP-syn flooding

availability



Client



SYN_{C1}

SYN_{C2}

SYN_{C3}

SYN_{C4}

SYN_{C5}

Server

Listening...

*Spawn a new thread,
Allocate buffers*

... and more

... and more

... and more

... and more

... and more

Hold on, won't 3-way handshake cause Client to receive it's own "syn flood" as server responds to all it's SYN's with SYN-ACK's?

Note asymmetric effort between attacker client and victim server

availability



TCP Connection Reset (DOS)

Each TCP connection (i.e each port) has an associated state sequence number

- ➡ An attacker can guess (sniff) the current sequence number for an existing connection and send packet with reset flag set, which will close the connection