Port scanning

~ confidentiality

- Using the "3-way" handshake, an attacker can scan for all open ports for a given host

  e.g. **`nmap`**

availability

TCP-syn flooding

Client

Server

SYN_{C1}

SYN_{C2}

SYN_{C3}

SYN_{C4}

SYN_{C5}

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