

# Port scanning

~ confidentiality

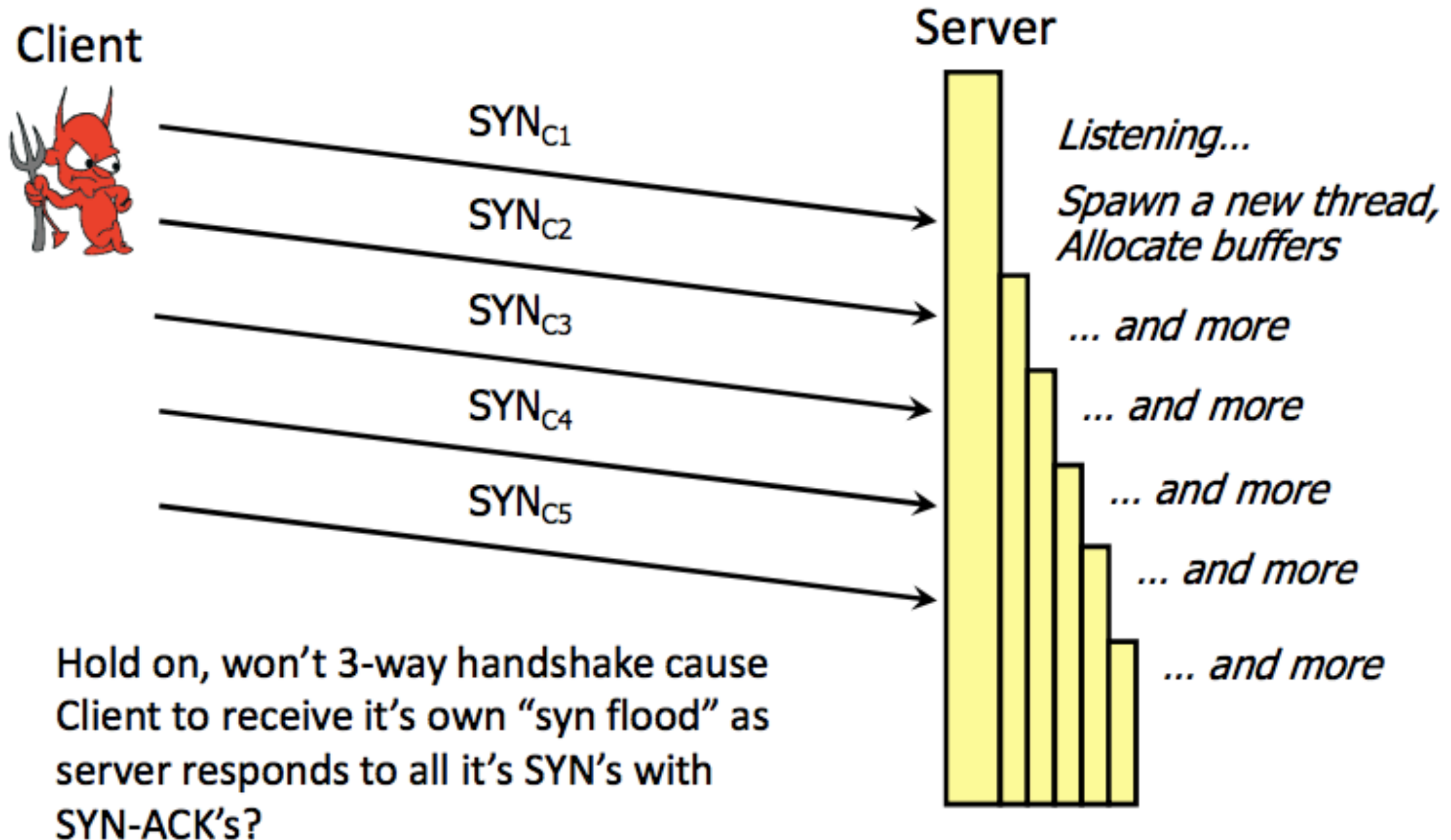


- ➔ Using the “3-way” handshake, an attacker can scan for all open ports for a given host

e.g. `nmap`

# TCP-syn flooding

availability



Note asymmetric effort between attacker client and victim server