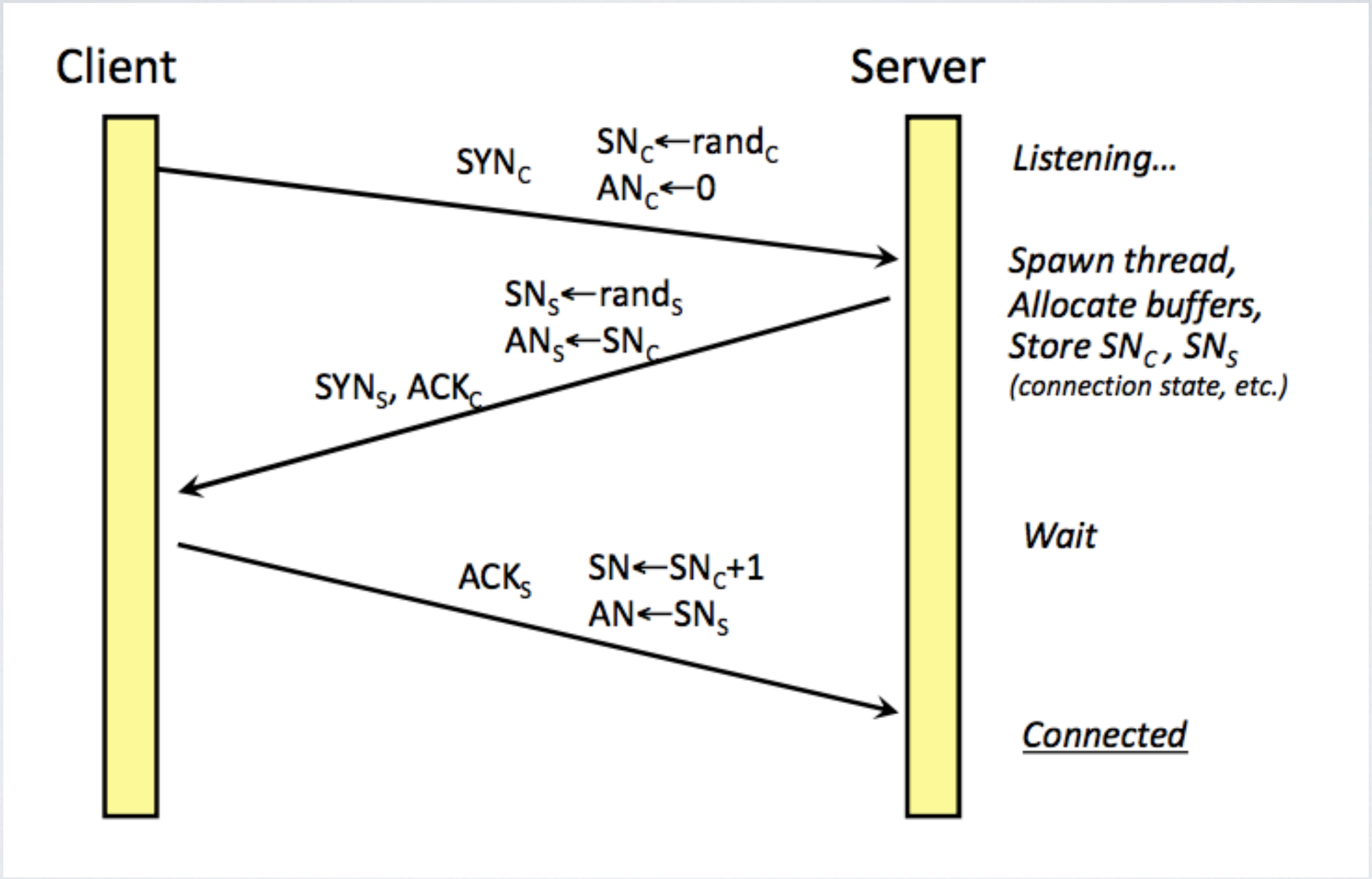
TCP "3-way" handshake




```
1 0.000000000   192.168.23.1     192.168.23.128   TCP      66 60645 → 8000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS
2 0.000069486   192.168.23.128   192.168.23.1     TCP      66 8000 → 60645 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
3 0.000758866   192.168.23.1     192.168.23.128   TCP      60 60645 → 8000 [ACK] Seq=1 Ack=1 Win=131328 Len=0
```

Port scanning

~ confidentiality

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

e.g. **`nmap`**

```
… 549.4… 192.168.2… 192.168.2… TCP  66 51467 → 8001 [SYN] Seq=0 Win=64240 Len=0 MSS=…
… 549.4… 192.168.2… 192.168.2… TCP  54 8001 → 51467 [RST, ACK] Seq=1 Ack=1 Win=0 Len…
```