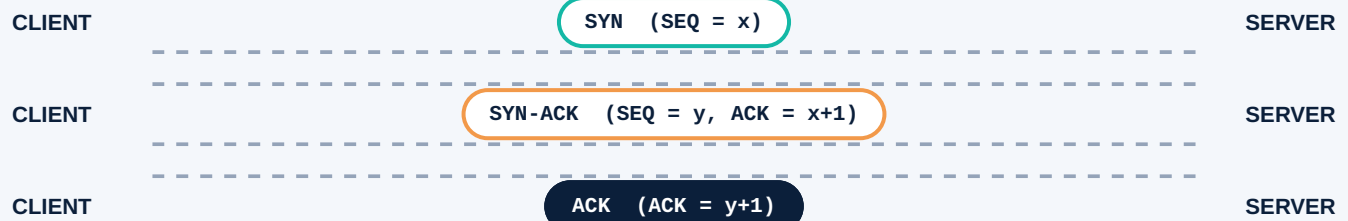




1 TCP THREE-WAY HANDSHAKE



2 KEY TCP FLAGS & SECURITY RELEVANCE

FLAG	PURPOSE	SECURITY NOTE
SYN	Starts connection	Used in SYN floods & stealth scans
ACK	Acknowledges data	Missing ACK often indicates scanning
RST	Abrupt termination	Used in RST injection attacks
FIN	Graceful close	Used in FIN scans
PSH / URG	Push / urgent data	Rarely normal together (Christmas tree)

3 COMMON HANDSHAKE ATTACKS

- **SYN Flood** → Half-open connections exhaust server resources
- **ISN Prediction / Session Hijacking** → Predictable sequence numbers allow takeover
- **TCP Split Handshake** → Simultaneous SYN evades stateful firewalls
- **RST Injection** → Spoofed RST kills legitimate sessions

4 ESSENTIAL WIRESHARK FILTERS

SYN only

```
tcp.flags.syn==1 and tcp.flags.ack==0
```

RST packets

```
tcp.flags.reset==1
```

Suspicious flags

```
tcp.flags.syn==1 and tcp.flags.fin==1
```

Specific stream

```
tcp.stream eq X
```

5 CORE DEFENSES

- ✓ SYN cookies
- ✓ Rate limiting of new SYNs
- ✓ Strong random ISN generation (RFC 6528)
- ✓ Stateful firewalls / SYN proxy
- ✓ Encrypted transport (TLS / IPsec) for session protection

6 QUICK PRACTICAL TIPS

- ▶ Always baseline your normal SYN-to-ACK ratio
- ▶ Watch for connections stuck in SYN_RECV
- ▶ Distinguish a graceful FIN close from an abrupt RST
- ▶ Practice with hping3 + Wireshark in a lab environment