TCP 3-Way Handshake — Interview & SOC Explanation

The TCP 3-way handshake is the process used to establish a reliable connection between a client and a server before any application data is exchanged.

Step 1: SYN (Client → Server)

The client sends a SYN packet to the server with an initial sequence number (Seq = x). This means: 'I want to start a connection and this is my starting sequence number.'

Step 2: SYN-ACK (Server → Client)

The server responds with SYN-ACK. It acknowledges the client's sequence number (Ack = x+1) and sends its own sequence number (Seq = y). This means: 'I received your request and I am ready to communicate.'

Step 3: ACK (Client → Server)

The client sends an ACK acknowledging the server's sequence number (Ack = y+1). After this step, the connection is established and data transfer can begin.

Why 3 Steps Are Required (Interview Critical)

- To confirm both sides are reachable
- To synchronize sequence numbers for reliable data transfer
- To prevent half-open connections
- To protect against spoofed connections

Security & SOC Perspective

- SYN flood attacks abuse Step 1 by sending excessive SYN packets
- Half-open connections are indicators of DoS attacks
- Network monitoring tools detect abnormal SYN/SYN-ACK ratios

One-Line Interview Answer

The TCP 3-way handshake ensures both client and server agree on sequence numbers and are ready for reliable, ordered communication before data transfer begins.