1. 4 bits
2. 6 flag bits.
   SYN,FIN,RST
3. The TCP three-way handshake connects a client and a server in three steps. First, the client sends a SYN packet with a sequence number to request a connection. The server replies with a SYN-ACK, confirming the request and sending its own sequence number. Finally, the client sends an ACK to confirm the server's response. After this, the connection is established, and data transfer can start.
4. If the final ACK does not arrive, the server will wait for a short time. It may resend the SYN-ACK in case the first one was lost. If there is still no response, the server will time out and close the connection. This prevents it from waiting forever.

5. Netstat -tna
6. In the output of the netstat -tna command, the keyword to identify half-open TCP connections is SYN_RECV. This means the server received a SYN request and sent a SYN-ACK but has not received the final ACK from the client. It indicates an incomplete connection, which could be due to network issues or a possible SYN flood attack.
7. netstat -tna | grep SYN_RECV | wc -l

8. In the TCP attack lab, SYN cookies are disabled on the victim machine to make it vulnerable to SYN flood attacks. Normally, SYN cookies prevent the system from holding half-open connections. By disabling them, the victim machine keeps these connections in the SYN_RECV state, allowing the attacker to overload its resources and simulate a denial-of-service attack.
9. The source IP addresses of the SYN packets depend on the attack method. If the attacker uses real IPs, the packets will show the attacker's actual IP address. If the attacker spoofs IPs, the packets will have fake, randomly generated IP addresses. Spoofing makes it harder for the victim to detect and block the attack.
10. The attack program is targeting Telnet, which uses port 23 for remote access. If the attack is successful, Telnet may become unresponsive due to too many half-open connections. However, SSH on port 22 and FTP on port 21 will not be directly affected unless the attack overloads the entire system.
11. sysctl -w net.ipv4.tcp_tw_recycle=0

    TCP cache allows the system to reuse connections instead of keeping many half-open connections, preventing resource exhaustion. This reduces the effectiveness of the SYN flood attack by clearing stale or incomplete connections quickly.
12.