20.1 Does an SYN flooding attack cause the victim server to freeze? Please explain why.

Yes, an SYN flooding attack can cause the victim server to freeze or become unresponsive. This happens because the server allocates resources (memory and connection state) for each incoming SYN request, but the attacker never completes the handshake. This exhausts the server's connection table, preventing legitimate users from connecting.

20.2 What will happen if the spoofed source IP address in a SYN flooding attack does belong to a machine that is currently running?

If the spoofed source IP belongs to a running machine, that machine will receive unexpected SYN-ACK packets from the victim server. If it responds with RST (reset) packets, the attack's effectiveness may be reduced since the victim server will clear those half-open connections.

20.3. An attacker launches a SYN flooding attack against the telnet server on a target machine. This particular telnet server listens to two ports, port 23 and port 8023. The attack is only targeting the default telnet port 23. When the attack is undergoing, can people still be able to telnet to the server using port 8023?

Yes, people can still telnet to port 8023. The SYN flood attack targets port 23 specifically, meaning port 8023 remains unaffected and is available for connections.

20.4 If TCP always uses a fixed sequence number (e.g., zero) in its SYN + ACK packet during the three-way handshake protocol, please describe how you can conduct a denial-of-service attack on the TCP server. Your objective is different from the SYN flooding attack: you want to cause the server to establish connections with many non-existing computers, thus exhausting the server’s resources, especially its memory.

If TCP always used a fixed sequence number, an attacker could send SYN requests with spoofed source IPs of non-existent machines. The server would then allocate resources for these connections, exhausting its memory and making it unable to handle legitimate requests. This results in a denial-of-service (DoS) condition.

20.5 All the information that a server needs to know about a connection is not only contained in the SYN packet but also in the final ACK packet from the client. Therefore, information-wise, there is no need to allocate a buffer to save the information about half-open connections. If we get rid of this buffer, the SYN flooding attack will not be effective anymore. Do you agree with such a statement or not? Please justify your answer.

The statement is incorrect. The server must maintain a buffer to track half-open connections because it needs to remember which SYN-ACK packets it has sent and wait for the final ACK from the client. Without this buffer, the server would be vulnerable to replay attacks and could not properly manage the TCP state.

20.6 To reset (RST) a connection between two remote machines, i.e., we will not be able to see the packets between these two machines, what are the main challenges?

The main challenge in resetting (RST) a connection between two remote machines is predicting the sequence number since the attacker must guess it correctly for the RST packet to work. Another challenge is that the attacker cannot see the packets between the machines, so they don't know the actual sequence numbers. Timing is also important because the RST packet must be sent at the right moment before the connection moves forward. Lastly, if the attacker is outside the network, firewalls and security settings might block the RST packet.

20.7 There is an active connection between a Telnet client (10.0.2.5) and a Telnet server (10.0.2.9). The server has just acknowledged a sequence number 1000, and the client has just acknowledged a sequence number 3000. An attacker wants to launch the TCP session hijacking attack on the connection, so he can execute a command on the server. He is on the same local area network as these two computers. You need to construct a TCP packet for the attacker. Please fill in the following fields:

- Source IP and Destination IP: (10.0.2.5, 10.0.2.9)
- Source port and Destination port: 23 (Telnet Port)
- Sequence number 3001 (3000 + 1)
- The TCP data field: Commands/Executions like stealing/deleting files.