1. SYN cookies help prevent SYN flooding by not allocating resources for SYN packets. Instead, they encode information in the SYN-ACK response and verify the ACK packet when it comes back. This way, they check if the connection is legitimate without storing state.

2. The proper way to close a TCP connection is the four-way handshake. One side sends a FIN packet, the other acknowledges with an ACK. Then, the second side sends a FIN, and the first side responds with an ACK to fully close the connection.

3. If the SYN+ACK packet reaches a real host, it will send a RST (reset) packet to the server because it never sent the original SYN request. This resets the connection and prevents it from being established.

4. The attacker gets the sequence number by sniffing network traffic or using techniques like predicting sequence numbers. If they are on the same network, they can capture packets directly.

5. The four elements that identify a TCP session are source IP, destination IP, source port, and destination port.

6. Along with those four elements, the sequence number must also be correct for a spoofed TCP packet to be accepted.

7. Commands in an attacker's program start with a new line to match the expected format of input in interactive sessions, ensuring they are properly processed.

8. When the attack works, the Telnet terminal freezes because the session is hijacked. TCP eventually closes the connection when no further data is received, ending communication between the client and server.