Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
One potential explanation for the website's connection timeout error message is: Mass amounts of SYN packets being sent to the server. The logs show that: There are numerous syn requests overflowing the server and it is overloaded This event could be: A denial of service attack (syn flood)

Section 2: Explain how the attack is causing the website to malfunction
When website visitors try to establish a connection with the web server, a three-way handshake occurs using the TCP protocol. Explain the three steps of the handshake: 1. Sending a SYN packet or synchronize request to the destination 2. The source returns a SYN/ACK or synchronize acknowledgement 2. Sending an ACK or acknowledgement packet from the souce to the destination Explain what happens when a malicious actor sends a large number of SYN packets all at once: The system starts struggling to keep up with the requests until it is overloaded and stops responding Explain what the logs indicate and how that affects the server: The logs indicate that the server was performing normal TCP/IP operations, until the number of SYN packet requests continued growing quicky, where it started to struggle before being entirely unable to respond to the requests.