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: TCP SYN Flood Attack The logs show that: Abnormal volume of TCP SYN requests. Unfamiliar IP address sending numerous SYN packets. Connection timeout errors reported. This event could be:

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.SYN (Synchronize): Initiating the connection, the client sends a SYN packet to the server, indicating it wants to establish a connection. 2. SYN-ACK (Synchronize-Acknowledge): The server responds with a SYN-ACK packet, acknowledging the client's request and indicating its willingness to establish a connection. 3.ACK (Acknowledge): The client sends an ACK packet, acknowledging the server's response. At this point, the connection is established. Explain what happens when a malicious actor sends a large number of SYN packets all at once:The malicious actor floods the server with a high volume of SYN packets without completing the handshake (i.e., without sending the final ACK). This overwhelms the server, tying up resources and preventing it from completing legitimate connections. Explain what the logs indicate and how that affects the server: Logs Indicate: Unusual SYN requests from an unfamiliar IP address. Abnormal volume of SYN packets. Server Impact:

The server becomes inundated, unable to distinguish between legitimate and malicious SYN requests.
Legitimate users experience connection timeouts as the server struggles to respond to the massive influx of SYN packets.
The server's resources are consumed, leading to a degradation in performance and eventual unresponsiveness.