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 a SYN flood attack.

The logs show that a large number of SYN packets are being sent from a single IP address, overwhelming the server's ability to handle legitimate requests.

This event could be a Denial of Service (DoS) attack, specifically a SYN flood, which causes the server to become unresponsive due to resource exhaustion.

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):
 The client (visitor) sends a SYN packet to the server to initiate a connection request. This step is intended to begin the process of establishing a communication channel.
2. SYN-ACK (Synchronize-Acknowledge):
 The server responds with a SYN-ACK packet to acknowledge the client's request and establish its willingness to communicate.
3. ACK (Acknowledge):
 The client sends an ACK packet back to the server, confirming that the connection is established, and the communication can begin.

The attacker floods the server with SYN packets, initiating connection requests without completing the handshake. The server responds with SYN-ACK packets but never receives the expected ACK, leaving connections half-open. This ties up server resources, causing it to become unresponsive and resulting in connection timeouts for legitimate users.

The logs show multiple SYN requests from the same IP, overwhelming the server and causing a denial of service (DoS).