Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption

The occurrence of a connection timeout error message on the website could possibly be attributed to a denial-of-service (DoS) attack. Analysis of the logs reveals that the web server becomes unresponsive due to an overwhelming influx of SYN packet requests. This occurrence aligns with a specific form of DoS attack known as SYN flooding.

Section 2: Explain how the attack is causing the website to malfunction

When attempting to establish a connection with the web server, website visitors engage in a three-way handshake using the TCP protocol. This handshake involves the following steps:

The source sends a SYN packet to the destination, requesting a connection.
The destination responds to the source with a SYN-ACK packet, indicating acceptance of the connection request and allocating resources for the source to connect.
The source sends a final ACK packet to the destination, acknowledging permission to establish the connection.
In the case of a SYN flood attack, an attacker deliberately inundates the server with a large volume of SYN packets simultaneously, overwhelming the server's available resources for connection reservations. Consequently, there are no remaining server resources to handle legitimate TCP connection requests.

The logs reveal that the web server has become overwhelmed, rendering it incapable of processing the SYN requests from visitors. As a result, the server cannot initiate new connections for incoming visitors, who consequently receive a connection timeout message.