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, a type of DoS attack. The logs show that the web server stops responding after it is overloaded with numerous SYN packet requests.

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

The website visitors initiate a three-way handshake with the web server using the TCP protocol. This handshake involves:

1. Sending a SYN packet from the visitor to the server to request a connection.
2. The server responds with a SYN-ACK packet to acknowledge the connection request and reserves resources.
3. The visitor sends a final ACK packet, confirming the connection.

However, during a SYN flood attack, a malicious actor floods the server with numerous SYN packets, depleting its resources and preventing it from processing legitimate connection requests. Logs show the server overwhelmed, unable to handle new connections, resulting in visitors receiving connection timeout messages.