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 **Denial-of-Service (DoS)** attack, more specifically a **SYN Flood** attack.

The logs show that:
A high volume of SYN packets were sent to the server without corresponding ACK responses, which is characteristic of a SYN Flood attack.

This event could be:
An attempt to exhaust the server's available resources by filling its connection table with half-open connections, ultimately causing a timeout error for legitimate users.

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. A **SYN packet** is sent from the source to the destination, requesting to initiate a connection.

2. The destination replies with a **SYN-ACK packet**, accepting the connection request and reserving resources for the connection.

3. A final **ACK packet** is sent from the source back to the destination, acknowledging the permission to connect.

Explain what happens when a malicious actor sends a large number of SYN packets all at once:
In a **SYN Flood attack**, a malicious actor sends a large number of SYN packets to the server, without completing the handshake. The server responds with SYN-ACK packets, waiting for the final ACK. Since the malicious actor never sends the ACK back, the server's connection table becomes filled with half-open connections, exhausting resources and rendering the server unable to handle legitimate requests.

Explain what the logs indicate and how that affects the server:
The logs indicate that the server is overwhelmed by the number of uncompleted connections, causing it to become unresponsive and leading to the timeout error experienced by legitimate users