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 Distributed Denial of Service (DDoS) attack, specifically a SYN flood attack, may have caused this network interruption.

The logs show that:
There is a high volume of SYN packets being received by the server, exceeding normal traffic levels. This influx likely overwhelms the server's ability to respond to legitimate connection requests.

This event could be:
A sign of a SYN flood attack, where a malicious actor sends an excessive number of SYN requests to the server, aiming to exhaust its resources and prevent legitimate users from connecting.

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 sends a SYN packet to the server to initiate a connection.
2. **SYN-ACK (Synchronize-Acknowledge):** The server responds with a SYN-ACK packet, acknowledging the request and indicating it is ready to establish a connection.
3. **ACK (Acknowledge):** The client sends an ACK packet back to the server, completing the handshake and establishing the connection.

Explain what happens when a malicious actor sends a large number of SYN packets all at once:
When a malicious actor sends a large number of SYN packets, the server receives more connection requests than it can handle. The server allocates resources to each request, waiting for the final ACK that never arrives. This leads to resource exhaustion, preventing legitimate users from completing the handshake and accessing the website.

Explain what the logs indicate and how that affects the server:

The logs indicate a significant spike in incoming SYN packets, suggesting a potential SYN flood attack. This flood of traffic causes the server to become overwhelmed, leading to connection timeouts for legitimate users, degraded performance, or even server crashes, as the server cannot process the volume of requests efficiently.