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** targeting the server.

The logs show that:
A significant number of incoming SYN packets are being received from one IP address, which suggests a SYN flood attack, a specific type of DoS attack.

This event could be:
An attempt by malicious actors to overwhelm the server's resources, preventing legitimate users from accessing the website.

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 (Synchronization)**: The client sends a SYN packet to the server, requesting to initiate a connection.

2. **SYN-ACK (Synchronization Acknowledgment)**: The server responds with a SYN-ACK packet, acknowledging the request and agreeing to establish the connection.

3. **ACK (Acknowledgment)**: The client sends an ACK packet back to the server, completing the handshake, and the connection is established.

Explain what happens when a malicious actor sends a large number of SYN packets all at once:
When a malicious actor sends numerous SYN packets but does not complete the handshake by responding with an ACK, the server allocates resources to maintain these half-open connections.
If enough half-open connections are maintained, the server's resources become exhausted, leading to its inability to process legitimate requests.

Explain what the logs indicate and how that affects the server:
The logs show a high volume of incoming SYN packets from one source, with very few or no corresponding ACK packets. This indicates a **SYN flood attack**.
This flood of incomplete connections saturates the server's connection queue, causing it to drop new incoming requests and leading to connection timeouts for legitimate users.