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: the server is slow and can’t finish connection.

The logs show that: the server is getting a lot of TCP SYN packets.

This event could be: a type of DoS called SYN flood attack.

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: source asking for a SYNchronization or connection

2. SYN-ACK: destination responding with an ACKnowledgement of the connection

3.: ACK: source acknowledging the connection is established

Explain what happens when a malicious actor sends a large number of SYN packets all at once: When the server is hit with a lot of SYN packets it tries to start a connection and it is waiting for ACK from the source but if no ACK is sent then the distination is waiting which consumes resources, so if a malicious actor send large number of SYN packets the server will be waiting and consuming resources with no resources left for legitimate connections which causes a Denial of Service (DoS).

Explain what the logs indicate and how that affects the server: logs indicate that the server is overwhelmed with SYN requests and it cant receive new connections.