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 DoS (Denial of Service) Attack.

The logs show that: The server has stopped responding as it is overloaded with SYN packet requests.

This event could be: A SYN Flood Attack. (A type of DoS 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. A SYN packet is sent from the source to the destination, requesting to connect.

2. The destination replies to the source with a SYN-ACK packet. (ACK) acknowledging the connection request and (SYN) to accept the connection request from the destination. The destination will reserve resources for the source to connect.

3. A final ACK packet is sent from the source to the destination acknowledging the permission to connect. Connection is established successfully.

Explain what happens when a malicious actor sends a large number of SYN packets all at once:

In the case of a SYN flood attack, a malicious actor sends a large number of SYN packets all at once, which overwhelms the server's available resources to reserve for the connection. When this happens, there are no server resources available for legitimate TCP connection requests and then the server starts to decline connection requests.

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

The logs indicate that the web server has become overwhelmed and is unable to process the visitors' SYN requests. The server is unable to open a new connection to new visitors so they receive a connection timeout message.