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 attack.The logs show that the server stops responding to request after its overloaded with SYN request.This event could be a SYN Flooding.

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.

2. (SYN/ACK) is the destination accepting the connection request.

3. The final ACK packet is sent from the source to the destinations, acknowledging the connections.

Explain what happens when a malicious actor sends a large number of SYN packets all at once. When a malicious actor uses a SYN flood, the actor is attempting to overload the server by forcing it to be taken offline or until it is unable to fulfill the request.

Explain what the logs indicate and how that affects the server. The logs indicate that is was overwhelmed due to very high SYN request by a threat actor causing the server not to perform actual SYN request from visitors.