Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption

The type of attack is a DOS attack using SYN flooding. This caused the website’s error timeout message since it was being flooded with SYN packet requests that ended up overwhelming the web server.

Section 2: Explain how the attack is causing the website to malfunction

When users attempt to connect to a web server, a three-way handshake takes place using the TCP protocol, involving the following steps:

The source sends a SYN packet to the destination, requesting a connection.
The destination responds with a SYN-ACK packet, accepting the connection request and allocating resources for the source to connect.
The source sends a final ACK packet to the destination, acknowledging the permission to connect.
However, a SYN flood attack occurs when a malicious actor floods the server with an excessive number of SYN packets all at once. This overwhelms the server's available resources to reserve for connections, leaving no room for legitimate TCP connection requests.

As a result, the server becomes overloaded, evident from the logs indicating an inability to process visitors' SYN requests. Consequently, new visitors experience connection timeouts since the server is unable to open new connections due to the resource exhaustion caused by the attack.