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: an unknown user is sending an DoS attack using the SYN flood attack, sending a lot of SYN requests making the server break down for not having the capacity to handle that number of requests.

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 attacker to the server, requesting to connect.

2. The destination replies to the source with an SYN-ACK packet to accept the request, the destination reserves resources for the source to connect.

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

In the case of an SYN flood attack, a malicious actor will send a large number of SYN packets all at once, this overwhelms the server's available resources. When this happens there are no resources left for legitimate TCP connection requests.

The log indicates that the web server has become overwhelmed and is unable to process the visitors' SYN requests.