Cybersecurity Incident Report

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

One possible reason for the website's connection timeout error message is a DDoS attack. The logs indicate that the web server becomes unresponsive when inundated with a barrage of SYN packet requests. This occurrence aligns with a form of DDoS attack known as SYN flooding.

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

When the website visitors try to establish a connection with the web server, a three-way handshake occurs using the TCP protocol. The handshake consists of three steps:

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 to accept the connection request. 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.

In the context of a DDoS attack, particularly a SYN flood attack, a malicious actor floods the server with an overwhelming number of SYN packets simultaneously. This flood of requests exhausts the server's available resources reserved for establishing connections. Consequently, there are no server resources left for legitimate TCP connection requests.

The logs indicate that the web server is inundated and unable to process the SYN requests from visitors. As a result, the server cannot open new connections for legitimate visitors, leading to a connection timeout message.