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 Denial-of-Service (DoS) attack. The logs show that the server received a large number of SYN packets from a single IP address which eventually caused it to stop responding. This event could be related to a type of Dos attack called 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. The steps for this are: 1. A SYN packet is sent from the source to the destination, this is a request to connect. 2. The destination address then replies with a SYN-ACK packet to acknowledge the request to connect and reserves resources ready for the connection. 3.A final ACK packet is then sent from the source to acknowledge permission to connect, after which, data can be transmitted. When a malicious actor conducts a SYN flood DoS attack, a large number of SYN packets are sent to the target in a short space of time. This overwhelms the server’s ability to allocate resources for legitimate TCP connections. The logs indicate that the server has become overwhelmed by the flood of SYN packets and is no longer able to process visitors’ SYN requests. This results in a connection timeout message being received by anyone who attempts to visit the site.