Analyze network attacks

Section 1: Identify the type of attack that may have caused this network interruption
One possible reason for the website's error message is a DoS attack. The logs show that the web server stopped responding after it was overloaded with SYN packet requests. This could be an example of 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, requesting to connect. 2. The destination replies to the source with a SYN-ACK packet and accepts the connection request. 3. A final ACK packet is sent from the source to the destination acknowledging the permission to connect. In a SYN flood attack, a malicious actor will send a large number of SYN packets all at once, overwhelming the server's resources to reserve for the connection. This ends with no server resources being left for legitimate TCP connection requests. The logs show that the web server has become overwhelmed and is unable to process the visitors' SYN requests. The server is unable to open a new connection to new visitors, showing the timeout message.