Analyze network attacks

Section 1: Identify the type of attack that may have caused this network interruption
A DoS attack is one theory as to why the website's connection timeout error message appeared. According to the logs, the web server stops responding when it receives too many SYN packet requests. This occurrence can be a SYN flooding DoS attack.

Section 2: Explain how the attack is causing the website malfunction
A three-way handshake using the TCP protocol takes place when website visitors try to connect with the web server. There are three steps to the handshake: 1. The source sends a SYN packet to the destination asking for a connection. 2. In order to accept the connection request, the destination responds to the source with a SYN-ACK packet. Resources will be set aside by the destination so that the source can connect. 3. The source sends the last ACK packet to the destination in order to confirm that the connection has been approved. A malicious threat actor will send several SYN packets all at once in a SYN flood assault, which overwhelms the server's resources it has set aside for the connection. When this occurs, no server resources are available for valid TCP connection requests. The logs show that the web server is overloaded and unable to handle SYN requests from visitors. When a new visitor encounters a connection timeout notice, the server is unable to establish a new connection.