Activity Exemplar: Analyze network attacks

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 DoS attack. The logs show that the web server is overwhelmed and stops working after receiving a large number of TCP SYN requests. This event could be a SYN flooding.

Section 2: Explain how the attack is causing the website 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 case of a SYN flood attack, the attackers send a large amount of number SYN packets to the server, making the server connection queue get filled up quickly having to hold information about the half-opened connection, unable to receive new legit requests. The logs indicate that the server is overwhelmed and can no longer receive new legitimate connection requests.