Activity Exemplar: Analyze network attacks

Section 1: Identify the type of attack that may have caused this network interruption
The website's connection timeout error message is most likely a Dos attack. The logs show that the web server stops responding after it is overloaded with SYN packet requests.It's a special type of Dos attack called SYN flood.

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, a malicious actor will send a large number of SYN packets all at once, which overwhelms the server's available resources to reserve for the connection. When this happens, there are no server resources left for legitimate TCP connection requests. The logs indicate 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 who receive a connection timeout message.