Activity: Analyze network attacks

Section 1: Identify the type of attack that may have caused this network interruption
A possible reason for encountering a connection timeout error on the website could be attributed to a Denial of Service (DoS) attack. According to the logs, the web server becomes unresponsive when it is overwhelmed by a barrage of SYN packet requests. This situation might correspond to a form of DoS attack known as SYN flooding.

Section 2: Explain how the attack is causing the website malfunction
When visitors of the website attempt to establish a link with the web server, they engage in a three-step handshake facilitated by the TCP protocol. This handshake is comprised of the following stages: The origin transmits a SYN packet to the destination, signaling a desire to establish a connection. In response, the destination issues a SYN-ACK packet back to the origin, signifying acceptance of the connection solicitation. Resources are allocated on the destination end to accommodate the forthcoming connection. To finalize the process, the origin dispatches an ACK packet to the destination, confirming the authorization to establish the connection. However, in scenarios involving a SYN flood attack, an adversarial entity executes a strategy wherein an extensive volume of SYN packets are dispatched simultaneously. This flood of packets overwhelms the server's resources, which are usually designated for reserving connections. Consequently, this resource depletion leaves no capacity to address authentic TCP connection entreaties. From the evidence in the server logs, it becomes evident that the web server is experiencing an attack, rendering it unable to effectively handle the SYN requests from legitimate visitors. This situation translates to the server's inability to initiate fresh connections for incoming visitors, resulting in those visitors encountering connection timeout notifications.