Activity: Analyze network attacks

Section 1: Identify the type of attack that may have caused this network interruption
The website timeout errors likely resulted from a DoS attack, specifically a SYN flooding attack. Server logs indicated the web server became unresponsive after being overwhelmed with SYN packet requests.

Section 2: Explain how the attack is causing the website malfunction
The website malfunction stems from exploitation of the TCP three-way handshake process. Normally, this process involves: 1. The source sends a SYN packet requesting connection 2. The destination responds with a SYN-ACK packet and reserves resources 3. The source confirms with an ACK packet to establish the connection In a SYN flood attack, attackers overwhelm the server by sending numerous SYN packets simultaneously, depleting the server's available resources for connection reservations. This prevents legitimate TCP connection requests from being processed, resulting in timeout messages for genuine visitors. The logs confirmed the server's inability to process new SYN requests due to resource exhaustion.