# Activity: Analyze network attacks

|  |
| --- |
| **Section 1: Identify the type of attack that may have caused this**  **network interruption** |
| The network interruption was caused by a TCP SYN flood attack. Wireshark logs show the server was overwhelmed by many SYN requests, which filled its connection queue and prevented legitimate users from connecting, resulting in timeout errors. |

|  |
| --- |
| **Section 2: Explain how the attack is causing the website malfunction** |
| When a visitor tries to connect to the website, a TCP three-way handshake is used to establish the connection:   1. The client sends a SYN packet to the server to request a connection. 2. The server replies with a SYN-ACK packet and reserves resources for the new connection. 3. The client responds with an ACK packet to complete the handshake.   In a SYN flood attack, an attacker sends a large number of SYN packets but does not complete the handshake. This fills up the server’s connection queue with half-open connections, using up its resources. As a result, legitimate users cannot connect to the server and receive timeout errors, which is confirmed by the server logs. |