# Activity Exemplar: Analyze network attacks

|  |
| --- |
| **Section 1: Identify the type of attack that may have caused this**  **network interruption** |
| One possible cause of the website’s connection timeout error is a Denial of Service (DoS) attack. Log analysis shows the web server becomes unresponsive after being flooded with excessive SYN packet requests, indicating a potential SYN flood attack.  SYN flood attack a type of DoS that overwhelms a server by exploiting the TCP handshake process. |

|  |
| --- |
| **Section 2: Explain how the attack is causing the website malfunction** |
| When visitors try to connect to the web server, a TCP three-way handshake is used:   1. The client sends a SYN packet to request a connection. 2. The server responds with a SYN-ACK, reserving resources for the connection. 3. The client replies with an ACK to establish the connection.   In a SYN flood attack, a malicious actor sends a high volume of SYN packets without completing the handshake. This exhausts the server’s resources, preventing it from handling legitimate connection requests.  Log analysis shows the server is overwhelmed and unable to process incoming SYN requests, resulting in connection timeout errors for legitimate users.  connection to new visitors who receive a connection timeout message. |