# Cybersecurity Incident Report

|  |
| --- |
| **Section 1: Identify the type of attack that may have caused this**  **network interruption** |
| One possible reason for the website’s connection timeout error is a DoS attack. The logs indicate that the web server ceases to respond after being overwhelmed with SYN packet requests, which may suggest a SYN flooding attack. |
|

|  |
| --- |
| **Section 2: Explain how the attack is causing the website to malfunction** |
| When website visitors attempt to connect to the web server, a three-way handshake occurs using the TCP protocol. This handshake involves the source sending a SYN packet to request a connection, the destination replying with a SYN-ACK packet to accept and reserve resources, and the source sending a final ACK packet to confirm the connection. However, if a malicious actor floods the server with a large number of SYN packets all at once, it overwhelms the server’s ability to reserve resources for legitimate connections. As a result, the server becomes unable to process legitimate connection requests, as indicated by the logs, leading to connection timeouts for new visitors. |