# Cybersecurity Incident Report

|  |
| --- |
| **Section 1: Identify the type of attack that may have caused this**  **network interruption** |
| After inspecting the log, the most likely reason for the server being unreachable/not responding is a Denial of Service (DoS) attack. The server is full of SYN, and SYN-ACK logs, which is most likely SYN Flooding. |
|

|  |
| --- |
| **Section 2: Explain how the attack is causing the website to malfunction** |
| When website visitors try to establish a connection with the web server, a three-way handshake occurs using the TCP protocol. Explain the three steps of the handshake:   1. A SYN packet is sent from the source to the destination, requesting a connection to the webserver. 2. The destination responds by SYN/ACK which means the destination has acknowledged the source. The destination will reserve resources for the   source to connect.   1. Finally the destination will send a packet called ACK which means the source has accepted the connection.     In case of a SYN flood attack, a malicious user sends countless SYN request to the server, overloading it to the point where the server does not have the bandwidth to keep up with the requests. As a result the server can’t process legitimate requests.  The logs show that the server is overwhelmed by the requests and can’t process further requests by visitors. The server is unable to open a new connection to new visitors as a result giving them a connection timeout error. |