# Cybersecurity Incident Report

| **Section 1: Identify the type of attack that may have caused this**  **network interruption** | |
| --- | --- |
| The logs show that the web server stops responding after it is  overloaded with SYN packet requests. So it is possible that it was a SYN flood DoS attack; malicious actors can take advantage of the TCP protocol by flooding a server with SYN packet requests for the first part of the handshake. That may cause slow down to the server or in this case interrupt the service. | |
|

| **Section 2: Explain how the attack is causing the website to malfunction** |
| --- |
| When the website visitors try to establish a connection with the web server, a  three-way handshake occurs using the TCP protocol. The handshake consists  of three steps:  1. A SYN packet is sent from the source to the destination, requesting to  connect.  2. The destination replies to the source with a SYN-ACK packet to accept  the connection request. The destination will reserve resources for the  source to connect.  3. A final ACK packet is sent from the source to the destination  acknowledging the permission to connect.  If the number of SYN requests is greater than the server resources available to handle the requests, then the server will become overwhelmed and unable to respond to the requests.  The logs indicate that the web server has become overwhelmed and is unable  to process the visitors’ SYN requests. The server is unable to open a new  connection to new visitors who receive a connection timeout message. |