# Cybersecurity Incident Report

|  |
| --- |
| **Section 1: Identify the type of attack that may have caused this**  **network interruption** |
| By analyzing the network logs in Wireshark, it can be seen that the server is getting attacked by a DoS. The logs shows that the server is overwhelmed by SYN packets from a malicious actor. |
|

|  |
| --- |
| **Section 2: Explain how the attack is causing the website to malfunction** |
| This attack takes advantage of three-way handshake in TCP protocol, when someone visits the website, a connection is made using three-way handshake. In this process a SYN packet is sent to the server and the server reserves some resources and replies with SYN-ACK packet while waiting for the source to send ACK packet.  In this case the attacker sent large number of SYN packets to consume all of the available server’s resources. The server is now unable to make any new connection causing the website to malfunction. |