# Cybersecurity Incident Report

| **Section 1: Identify the type of attack that may have caused this**  **network interruption** | |
| --- | --- |
| This could potentially by a DDoS, Dos, or a SYN flood attack, otherwise it could be a temporary outage issue. However the logs from the server show that it is being overwhelmed by a large amount of SYN requests which leads me to believe that this must be a SYN flood attack from a threat actor. | |
|

| **Section 2: Explain how the attack is causing the website to malfunction** |
| --- |
| When you visit a website via TCP a three way “handshake” occurs. The client first sends SYN packets to the host, the host will then send back SYN/ACK packets to acknowledge the SYN packet. The client will then send back a ACK packet to finalize the connection  However when a server receives a large amount of SYN packets in a short amount of time the server will then be too busy and too overloaded to respond to any legitimate requests as it is trying to process all the SYN packets.  The logs indicated a large amount of SYN packets being directed at the server which has caused it to stall out and be unable to respond to legitimate traffic. This server houses the website that has all of the travel packages that we sell to customers. The attack has made them unable to access the site and thus unable to sell any packages as the attack was going on. |