# Cybersecurity Incident Report

| **Section 1: Identify the type of attack that may have caused this**  **network interruption** | |
| --- | --- |
| The network is potentially experiencing a website’s connection timeout error message is a DoS attack. The wireshark packet sniffer tool shows with the logs that the web server stops responding after it is overloaded with SYN packet requests. | |
|

| **Section 2: Explain how the attack is causing the website to malfunction** |
| --- |
| The wireshark packet sniffer tool indicates that there is an overload of packages being sent into the server from the same IP address. For this reason, the server is having a difficult time having the ability to respond to the abnormally large number of SYN requests, due to being overwhelmed. These symptoms indicate that this is an SYN flood attack As the visitors try to establish a connection with the server, utilizing the TCP protocol’s handshake via Requesting to connect with SYN. Then, the destination replies to the source with a SYN-ACK packet to acknowledge the connection. Finally, the source will send the ACK back to confirm the permission to connect with the destination.  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. Which is exactly the description of a SYN flood attack.SYN flood attack consists of overwhelming the server’s resource, in order to leave the server with no resource to be able legitimate TCP connection requests, leaving it open for more attacks. |