# Cybersecurity Incident Report

| **Section 1: Identify the type of attack that may have caused this**  **network interruption** | |
| --- | --- |
| A connection timeout error message is an indication that the server is not responding. And after using a packet sniffer to investigate the problem, a large number of TCP SYN requests came from an unfamiliar IP address. This event could be a DoS attack, specifically a SYN flood attack and a high probability combination of IP spoofing. | |
|

| **Section 2: Explain how the attack is causing the website to malfunction** |
| --- |
| The attack is flooding the server with SYN requests and if the SYN requests overwhelms the server, it will shut down.  A TCP 3-way handshake:   1. A device will send a SYN request to the server 2. The server will respond with a SYN/ACK packet 3. To complete the handshake, the device will send the ACK packet   SYN flood attack works like imitating a TCP handshake by sending SYN requests to the server but in large volume in a short amount of time  The logs indicate that the server is being overwhelmed by receiving SYN requests in a shorter amount of time than normal TCP 3-way handshake. |