# Cybersecurity Incident Report

| **Section 1: Identify the type of attack that may have caused this**  **network interruption** | |
| --- | --- |
| DoS is probable, since many SYN packets are being sent to the server. It is likely not a DDos, since the packets are being sent from the same ip. The site is taking a long time to load and report connection timeouts because the server can’t handle the continuous SYN packets being received. | |
|

| **Section 2: Explain how the attack is causing the website to malfunction** |
| --- |
| The attack is made up of many SYN packets being sent to the server from the same ip. The TCP/HTTP logs show about 200 SYN packets sent in less than a minute. Since the server is being flooded, employees and customers are unable to access the website, causing the transactions to cease and the reputation of the website to fall. |