# Cybersecurity Incident Report

| **Section 1: Identify the type of attack that may have caused this**  **network interruption** | |
| --- | --- |
| The network interruption experienced on our website likely resulted from a SYN flood attack, as indicated by a surge of TCP SYN requests originating from an unfamiliar IP address. This form of attack inundates our web server with incomplete connection requests, overwhelming its resources and impeding its ability to handle legitimate user connections effectively. | |
|

| **Section 2: Explain how the attack is causing the website to malfunction** |
| --- |
| During a three-way handshake, a legitimate connection is established through a series of steps: first, a client sends a SYN packet to the server, which responds with a SYN-ACK packet, and finally, the client sends an ACK packet to complete the process. In a SYN flood attack, a malicious actor exploits this process by sending an excessive number of SYN packets without completing the handshake. As a result, the server allocates resources for each unfulfilled request, leading to resource exhaustion, connection delays, and eventual service disruption for legitimate users attempting to access the website. This prompted us to temporarily take the server offline and implement IP blocking as an initial countermeasure. |