# Cybersecurity Incident Report

|  |
| --- |
| **Section 1: Identify the type of attack that may have caused this**  **network interruption** |
| One potential explanation for the website's connection timeout error message is: There is a large number of TCP SYN request from an unfamiliar IP address indicating a flood of incoming traffic trying to establish a connection with the server  The logs show that: there was a high volume of SYN requests being sent to the server from an unfamiliar address, overwhelming the server’s capacity to respond  This event could be: a SYN flood attack which is a type of DDoS attack |
|

|  |
| --- |
| **Section 2: Explain how the attack is causing the website to malfunction** |
| When website visitors try to establish a connection with the web server, a three-way handshake occurs using the TCP protocol. Explain the three steps of the handshake:  1. The first step is for the client to send a SYN message to request connection  2. Then the server responds with SYN/ACK to acknowledge the receipt of the client’s request and leaves a port open  3. The server receives the ACK packet and a TCP connection is established  Explain what happens when a malicious actor sends a large number of SYN packets all at once: The server will be overwhelmed and become unable to function leading to a denial of service as it cannot process legitimate requests  Explain what the logs indicate and how that affects the server: the logs show an abnormally high number of incoming SYN packets which consumes server resources and bandwidth, preventing the server from servicing legitimate traffic and causing connection timeouts and service disruptions |
|  |