# Cybersecurity Incident Report

**Made By: NIDA AZAM**

|  |
| --- |
| **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:  Too many requests overwhelmed the server, leaving no resources for the legitimate users.  The logs show that:  Too many TCP SYN requests from unfamiliar IP address.  This event could be:  A SYN flood attack which is a type of DOS (Denial of Service) 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. First the client sends SYN requests to server   2. Then server responds with SYN-ACK.   1. Client completes the connection with ACK request.   Explain what happens when a malicious actor sends a large number of SYN packets all at once:  When a malicious actor sends large number of SYN packets then the server gets busy in those fake requests and keeps waiting for final ACK. This overloads the server and no resources are left for legitimate users.  Explain what the logs indicate and how that affects the server:  The logs indicate repeated SYN requests that were never completed. It shows half-open connection due to which server resources are being used and not available for the real traffic. |