# 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: that the server is overwhelmed and cannot respond to the requests.  The logs show that: there’s a large number of TCP SYN requests coming from an unknown IP address.  This event could be: a SYN flood attack to the web server from a malicious actor, causing a network level direct Denial of Service (DoS). |
|

|  |
| --- |
| **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. In the first step of the handshake, a SYN (synchronize) packet is sent to the server to initiate the connection.  2. When the server receives the packet, it validates the packet by sending back a SYN/ACK packet to confirm that the web server will reserve resources for this request.  3. When the host receives the confirmation, then an ACK packet is sent to the server to establish the TCP connection and start transmission.  Explain what happens when a malicious actor sends a large number of SYN packets all at once:  When a malicious actor sends a large number of SYN packets all at once, it tries to flood the server by simulating multiple TCP connections. The server is then overwhelmed by so many requests, causing a DoS (Denial of Service).  Explain what the logs indicate and how that affects the server:  The logs indicate that there’s a large number of TCP SYN requests coming from an unknown IP address, and this is likely causing the server to be overwhelmed. When the server is flooded, it starts consuming all the available resources to respond to all the requests, eventually giving timeout errors to anyone trying to connect to the website. This unknown IP address is identified in all the logs tagged in red, this indicates that it’s a direct network level Denial of Service (DoS) attack.  To prevent this attack happening in the future, I suggest improving the configuration of the firewall. |