# 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:  The logs show that: **large number of TCP SYN requests coming from an unknown IP address.**  This event could be: **Possible TCP SYN DOS 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. **Synchronization request sent to the destination server requesting a connection**  2. **Acknowledge and Synchronization reply from destination server to requested host to accept the connection.**  3. **Acknowledge from the requested host that reply from the destination server was received.**  Explain what happens when a malicious actor sends a large number of SYN packets all at once: **The server replies to each SYN request and waits for response from the source. Each new request is processed until limits of memory/CPU or the SYN requests take over all the ability for the server to process and respond other requests that are sent.**  Explain what the logs indicate and how that affects the server: **Logs indicate that a large number of incoming SYN request have been directed at the server. We can see that proper handshake was completed by a few requests. A large number of SYN were sent from a single IP address 203.0.113.0 and no return Acknowledgement from the IP address was returned. Suggested that a firewall be placed in front of the server to filter SYN DOS and DDOS attacks against the companies website server.** |