# 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 are to many SYN requests coming in.  The logs show that: Port 443 is receiving too many SYN requests from IP address 203.0.113.0.  This event could be: A 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. The source client sends a SYN packet requesting connection.  2. The destination sends back a SYN/ACK packet accepting the connection with the source.  3. The source client then sends back the ACK packet establishing the connection with acknowledgement.  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, it will eventually overwhelm the destination as it will run out of response ports.  Explain what the logs indicate and how that affects the server: The logs indicate that a malicious actor with the IP address of 203.0.113.0 has been sending a large number of SYN packets requesting connection all at once. This in turn is causing available resources to be taken up quickly, leaving no resources to be used for legitimate TCP requests. The server was unable to handle all the requests and in turn was unable to create a new connection, causing users to receive a timeout message. |