# 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 multiple SYN requests made within short periods of time, and they are most likely causing the connection timeout error.  The logs show that: multiple SYN requests are made by 203.0.113.0  This event could be: a typical SYN flood attack, aka 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. SYN from the client   This is an initial request from the client device trying to access the server. SYN stands for synchronize.   1. SYN ACK from the server   This is the response from the server that shows the server acknowledges the SYN request. ACK stands for acknowledge.   1. ACK from the client   This is the final response from the client that the client acknowledges the permission to connect to the server.  Explain what happens when a malicious actor sends a large number of SYN packets all at once: when multiple SYN packets beyond the limits of the server are sent at once, the server fails to respond to the requests and results in a timeout or a crash.  Explain what the logs indicate and how that affects the server: log 73, 80, 85, 92, 121 shows RST, ACK packet, which indicates normal users from different IP addresses are experiencing a timeout. Log 77 also shows 504 Gateway Time out error sent to the user. |