# 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 SYN messages are received by the server  This event could be: Smurf Attack with SYN flooding 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 Device sends a SYN signal to the server  2. The server responds with SYN/ACK Signal  3. Once the device receives SYN/ACK signal , it responds back with Ack Signal and thus establishing TCP/IP Connection B/W device and Server  Explain what happens when a malicious actor sends a large number of SYN packets all at once: When Large number of SYN packets is flooded to the server , the Server responds back with SYN/ACK repeatedly consuming the bandwidth , this in turn cause delay in incoming and outgoing traffic and in the end crashes the server if it’s not intervened  Explain what the logs indicate and how that affects the server: Wireshark log |