# 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:  This event could be: |
|

**One potential explanation for the website’s behavior is a DoS attack, as the**

**The system is receiving a time out error message, followed by the logs showing multiple attempts in quick succession starting at log entry number 47, Wireshark was started it then proceeded to pick up 47 messages within 3 seconds after starting the log. Looking at the log it appears to be a SYN flood 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. **a SYN packet is sent from the source to the destination requesting to connect to the intended server/system.**  2. **the destination then receives the SYN packet and replies to the source with at SYN-ACK packet to accept the intended connection request. The system will then save the intended resources received to help make future connections quicker.**  3. **the ACK packet is then from the Source back to the destination acknowledging the permission to connect to the system.**  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 at once it causes the destination target to be flooded and overwhelmed causing it to shut down, preventing new legitimate TCP connection requests from being made.**  Explain what the logs indicate and how that affects the server: **the log server indicates that the server has become overwhelmed from multiple visitor SYN requests. The server is unable to open new visitor requests to be met by a Timeout Message for users.** |