# 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 a Dos attack.  The logs show that: The logs show that the web server stops responding after it is  overloaded with SYN packet requests.  This event could be: This event could be a type of DoS attack  called SYN flooding |
|

|  |
| --- |
| **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(Synchronize): The client sends a **SYN** (synchronize) packet to the server to initiate the connection.  2. SYN-ACK: The server receives the SYN packet and responds by sending a **SYN-ACK**(Synchronize-acknowledge) packet back to the client.  3.ACK: The client receives the SYN-ACK packet from the server and responds with an **ACK**(acknowledge) packet.  Explain what happens when a malicious actor sends a large number of SYN packets all at once: It can result in a **SYN flood attack**, which is a form of **Denial of Service (DoS)** or **Distributed Denial of Service (DDoS)** attack. The goal of this attack is to overwhelm a target server by exhausting its resources, preventing legitimate users from establishing connections.  Explain what the logs indicate and how that affects the server: As you scroll through the rest of the log, you will notice the web server stops responding to legitimate employee visitor traffic. The visitors receive more error messages indicating that they cannot establish or maintain a connection to the web server. From log item number 125 on, the web server stops responding. The only items logged at that point are from the attack. As there is only one IP address attacking the web server, you can assume this is a direct DoS SYN flood attack. |