# 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: Potential DoS or DDoS attack  The logs show that: There seems to be a consistent stream of requests SYN happening on the server from outside of the company & from one concentrated location  This event could be: Likely a DoS attack, specifically a SYN flood | |
|

| **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 first step of the handshake is the synchronize (SYN), this is the initial contact that is made on the network for anyone to request something  2. Followed by the initial SYN is the response given known as acknowledge (ACK), this is the servers way of letting a connection know that it received the request and will then determine what to do with it. Like the first step if the request goes through the response will be labeled as SYN ACK which is telling the initial source that it has accepted the request and is sending your info back to you  3.Once the first 2 steps have occurred the final step is another ACK, which is the final confirmation and will then give the information requested  Explain what happens when a malicious actor sends a large number of SYN packets all at once: The server will begin to slow down and not be able to handle the incredibly fast & huge multitude of requests being sent to it, eventually slowing it to the point of total disconnection  Explain what the logs indicate and how that affects the server: The logs indicate that one individual was flooding the server with nothing but SYN requests to eventually bring down the entire website, there’s also information in the logs that points to an employee IP being used. Either the individual is compromised or they have become a rogue employee. |