# Cybersecurity Incident Report: DoS attack

| **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 web server is not responding because it may be overwhelmed  The logs show that: A repeated number of SYN requests are originating from a single IP address. Legitimate requests from employees are unable to be processed by the web server as it may be overwhelmed.  This event could be: A Denial of Service (DoS) attack | |
|

| **Section 2: 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: The originator of the connection request sends its information along with a connection request 2. SYN/ACK: The recipient of the connection request sends an acknowledgement of the connection request, along with its information. 3. ACK: The originator of the connection request acknowledges the new connection   When the malicious actor sends a large number of SYN packets all at once, the web server becomes overwhelmed by the number of new connection requests.  The logs indicate that while the web server attempts to make connections at first, it quickly becomes overwhelmed and no longer has the resources to create new connections, or maintain existing ones. |