# 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: An abnormal number of SYN requests coming in at a rapid pace from a single IP, that causes the web server to stop responding.  This event could be: 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. A SYN packet is sent from the source to the destination, wanting to connect. 2. The destination replies to the source with a SYN-ACK packet which accepts the connection. Destination reserves resources for the source to connect 3. Final ACK packet is sent from the source to the destination as an acknowledgement for the permission to connect   Explain what happens when a malicious actor sends a large number of SYN packets all at once: When a large number of SYN packets is sent all at once it overwhelms the server’s available resources to reserve for connection. Leaving no resources for legitimate TCP connection requests  Explain what the logs indicate and how that affects the server: Log indicates that the server has become overwhelmed and is unable to process visitors’ SYN request. This is shown as the employees are no longer able to connect. Legitimate visitors receive a connection timeout message. |