# 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:**  that the web server is experiencing a SYN flood attack, a type of Distributed Denial of Service (DDoS) attack.  **The logs show that:**  There is an abnormally high number of TCP SYN requests originating from an unfamiliar IP address. This indicates that a malicious actor may be attempting to overwhelm the server with fake connection requests, causing it to exhaust its available resources.  **This event could be:**  part of a coordinated attack designed to make the website unavailable to legitimate users by overloading the server's ability to process incoming connection requests. |
|

|  |
| --- |
| **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 a new TCP connection.    2. SYN-ACK (Synchronize-Acknowledge): The server responds with a SYN-ACK (synchronize-acknowledge) packet, acknowledging the receipt of the SYN packet from the client.  3. ACK (Acknowledge): The client sends an ACK (acknowledge) packet back to the server to confirm the connection. Once this step is completed, a full TCP connection is established, and data can be exchanged.  **Explain what happens when a malicious actor sends many SYN packets all at once:**  When a malicious actor sends many SYN packets all at once, the server allocates resources to respond to each SYN request by sending back SYN-ACK packets. However, if the attacker does not send the final ACK packet needed to complete the three-way handshake, the server keeps these partially open connections in a backlog queue, waiting for the connection to complete.  This backlog queue has a limited size, and when it fills up with these half-open connections (also known as half-open or half-closed connections), the server is unable to accept new legitimate connection requests. This results in legitimate users experiencing connection timeouts and being unable to access the website.  **Explain what the logs indicate and how that affects the server:**  The logs indicate a high volume of incoming SYN requests from an unfamiliar IP address, which suggests a SYN flood attack. The server, overwhelmed by these fake connection attempts, is unable to process legitimate traffic. This overload causes the server to use up its resources, leading to delayed responses or complete connection failures, and ultimately results on the website being inaccessible to legitimate users. This attack not only disrupts service availability but also potentially impacts the company’s business operations and reputation. |