# 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 SYN flood attack.  The logs show that:   * There is a large number of TCP SYN requests coming from an unfamiliar IP address. * The server is being overwhelmed by the volume of incoming SYN requests, leading to a connection timeout error when legitimate users try to access the site.   This event could be:  A Denial of Service (DoS) attack, specifically a SYN flood, which exploits the TCP handshake process to overload the server’s resources. |
|

|  |
| --- |
| **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: The client (visitor) sends a TCP SYN packet to the server, indicating a request to establish a connection. 2. SYN-ACK: The server responds with a TCP SYN-ACK packet, acknowledging the request and indicating that it’s ready to complete the connection. 3. ACK: The client sends back a TCP ACK packet, confirming that the connection has been successfully established, and the data exchange can begin.   Explain what happens when a malicious actor sends a large number of SYN packets all at once:   * The attacker sends an overwhelming number of SYN requests to the server, often with spoofed IP addresses, so the server never receives the corresponding ACK packets to complete the handshake. * The server allocates resources (e.g., memory and processing) for each half-open connection, waiting for the final ACK. Since the attacker doesn’t send the ACK, the server’s resources are exhausted, preventing legitimate users from establishing connections and causing the server to become unresponsive.   Explain what the logs indicate and how that affects the server:   * The logs show an abnormal increase in SYN requests coming from an unfamiliar IP address. This indicates that the server is being targeted by a SYN flood attack. * As the server attempts to process these excessive SYN requests, it runs out of resources (e.g., connection slots, memory), causing timeouts for legitimate visitors and making the server slow or completely unresponsive. This leads to the connection timeout error that user experience when trying to access the website. |
|  |