# Cybersecurity Incident Report

|  |
| --- |
| **Section 1: Identify the type of attack that may have caused this**  **network interruption** |
| The website connection timeout error is likely caused by a Denial of Service (DoS) attack known as SYN flooding. As a result, users' requests cannot be processed, causing disruptions and timeouts. |
|

|  |
| --- |
| **Section 2: Explain how the attack is causing the website to malfunction** |
| The website uses the TCP protocol for communication, which involves a three-way handshake process when a user tries to connect. First, the user sends a SYN (synchronization) request to the server. The server then responds with a SYN-ACK (synchronization-acknowledgment) packet. Finally, the user sends an ACK (acknowledgment) packet back to the server, establishing the connection.  In a SYN flood attack, the attacker exploits this three-way handshake by sending an extremely high volume of SYN requests to the server, overwhelming its capacity to respond effectively. Instead of completing the handshake process by sending ACK packets, the attacker either sends forged source IP addresses or simply does not respond further. As a result, the server keeps waiting for ACK packets and ends up with numerous half-open connections that consume valuable resources.  The logs analyzed using Wireshark have provided valuable evidence of a potential SYN flood attack. The presence of a significant number of SYN requests originating from the same IP address in a short period strongly indicates that the server is under attack.  Due to the attack's overwhelming nature, the server's resources become exhausted, making it unable to handle legitimate user requests properly. This leads to slow response times and eventually causes website malfunctions, connection timeouts, or even complete unavailability of the website's services for genuine users.  To mitigate the impact of such attacks, network administrators should implement security measures like rate-limiting, SYN cookies, and traffic filtering to identify and block malicious SYN requests, ensuring the website remains stable and accessible to legitimate users. |