# Cybersecurity Incident Report

|  |
| --- |
| **Section 1: Identify the type of attack that may have caused this**  **network interruption** |
| The website's connection timeout error may be due to an overwhelming SYN request, potentially indicating a SYN flood attack. The logs reveal an HTTP/1.1 504 Gateway Time-out error, suggesting that the gateway server waited too long for a response from the web server. Additionally, an [RST, ACK] packet was observed, which is sent when the [SYN, ACK] packet isn't received by the web server, resulting in a timeout error for the visitor. This situation aligns with the characteristics of a SYN flood attack, a type of DoS attack that floods a server with simulated TCP/IP connections using SYN packets. In such an attack, the server may struggle to handle the excessive connection requests, leading to timeouts and connection issues. |
|

|  |
| --- |
| **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. The user request acknowledgement or access from the server, it sends a synchronize for the server to acknowledge.  2. The server then acknowledges the synchronize request from the user.  3. After the handshake occurs, the server then sends an acknowledgement where it gives user access to the website.  Explain what happens when a malicious actor sends a large number of SYN packets all at once: The server gets overwhelmed when there is large amount of SYN packets to receive. It will not load or function as it is intended. The legitimate website visitors will be able to access the site.  Explain what the logs indicate and how that affects the server: The logs indicate that there are too many SYN packets request and there are no acknowledgement happening. Flooding the servers with requests that are unable to be answered. |