# Cybersecurity Incident Report

|  |
| --- |
| **Section 1: Identify the type of attack that may have caused this**  **network interruption** |
| Upon a thorough analysis of the TCP and HTTP logs using the network analyzer tool Wireshark, it has been determined that the company's website fell victim to a Denial of Service (DoS) attack. Specifically, this attack took the form of a SYN flood, which effectively depleted all the resources responsible for handling legitimate user requests. This resource exhaustion ultimately resulted in a denial of service for authentic users.  The investigation further revealed that a single IP address was responsible for flooding the port, confirming the nature of the attack as a DoS attack. |

|  |
| --- |
| **Section 2: Explain how the attack is causing the website to malfunction** |
| Prior to the attack, when visitors attempted to access the website and initiate a connection via TCP, the server successfully executed a three-way handshake. However, as the attacker initiated the SYN flood attack, the response time for visitors began to experience slight delays, measured in milliseconds. With the increasing volume of SYN packets from the attacker, the server's ability to establish connections with legitimate requests was compromised, as the port ceased to listen to visitor requests.  As visitors awaited the arrival of the ACK Packet, which never materialized due to the attack, they were presented with a "bad gateway" error message, signifying that the server was taking an extended period to respond. As the attack persisted and the port became inundated with packets, the server eventually ceased responding altogether.  To mitigate the attack while the DoS attack is ongoing, it is imperative to take specific measures. Firstly, the offending IP address responsible for the attack should be blocked. Secondly, the firewall should be configured to scrutinize whether the source IP address matches any of the destination's private IPs. If such a match is detected, it should be blocked, as it could potentially be a spoofed IP address employed by the attacker. |