# Cybersecurity Incident Report

|  |
| --- |
| **Section 1: Identify the type of attack that may have caused this**  **network interruption** |
| After analyzing the TCP and HTTP log using the network analyzer tool Wireshark, it was concluded that the company’s website has encountered a DoS attack. It is a SYN flood attack which has exhausted all the resources responsible for responding to the authentic users leading to denial of service.  As there is one IP address responsible for flooding the port, it is DoS attack. |
|

|  |
| --- |
| **Section 2: Explain how the attack is causing the website to malfunction** |
| Before the occurrence of the attack, when the visitors were trying to access the website and establish connection via TCP, the server was establishing a successful three-way handshake. As the attacker started the SYN flood attack, the response time to the visitors started to get delayed by some milliseconds, and as the SYN packets sent by the attacker started to increase, the server was unable to establish connection with the legitimate requests as the port was no longer listening to the visitor’s request. As the visitor waited for the ACK Packet and it didn’t arrive, the users were shown the error of bad gateway as the server was taking too long to respond. As the attack continued and the port was flooded with packets, the server finally stopped responding. To mitigate the attack while the DoS attack is in play, the specific IP should be blocked and the firewall should be configured to see if the source’s IP address matches any of the destination’s private IP, and if it does then it must be blocked as it can be the spoofed IP. |