# Cybersecurity Incident Report

| **Section 1: Identify the type of attack that may have caused this**  **network interruption** | |
| --- | --- |
| Our web server Overwhelmed with volume of incoming traffic , the log show that an unfamiliar Ip adresse adresse is sending multiple TCP SYN packets, and this event could be a dos Attack known as SYN flood attack. | |
|

| **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- First the client send a SYN packet to the web server  2. The web server then respond with a SYN/ack  3. After that the client sends an ACK packet which establishes the connection.  But when a malicious attacker send multiple SYN packet to the server, they overwhelm the server with the number of SYN packets which cause the server to go down and stop functioning , the logs show a big volume of SYN packets from an unfamiliar IP, I took the website down and blocked this unfamiliar IP but this will only last a short time before attackers figure it out and use another IP adresse. |