# Cybersecurity Incident Report

|  |
| --- |
| **Section 1: Identify the type of attack that may have caused this**  **network interruption** |
| One potential explanation for the website's connection timeout error message is a SYN flooding DoS attack. The logs show that the attack is performed from a single IP address “203.0.113.0”. It can be seen that the attack caused a legitimate user with the IP address “192.0.2.1” to not be able to connect to the site. Right after that it can be seen that the suspicious IP floods with SYN requests blocking the server. |
|

|  |
| --- |
| **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. In the first step, the client sends a [SYN] synchronization request to the server. In the second step, if the server approves the connection, it sends a [SYN, ACK] to inform the client about acknowledgement. After this, a final ACK packet is sent from client to the server acknowledging the permission to connect.  When a malicious actor sends a large number of SYN packets all at once, the server floods with requests and cannot get any other packets from other clients. This causes the server to malfunction, thus the other requests do not even reach the server and die from timeout.  The logs help cybersecurity analysts analyze the web traffic on a connected router. The logs in this situation shows us that in the first couple of minutes, some legitimate connections were done, but as the attack progressed the server started to reject legitimate users and cause issues. After a couple of more minutes, the server was flooded with SYN requests from a specific IP address causing others to access the website. |