# 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 that the server is flooded by SYN requests from one IP address.  The logs show that the IP number 203.0.113.0 is requesting to synchronize with the web server to create a TCP handshake. However, the request is not done when the server sends the acknowledgement and the IP persists to send SYN request, until the whole server activity is flooded with the same request.  This event could be a DoS attack, since usual connections don’t send this many SYN requests. Also, it is not a DDoS attack, because only one IP address is responsible for the requests and flooding 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. Explain the three steps of the handshake:   1. The visitor send a SYN request to the server 2. The destination server sends a SYN-ACK to say it has acknowledged the visitor, and the visitor has permission to send other requests. Here, the server waits for an ACK message from the source. 3. The source sends an ACK message to the destination to say it has acknowledged the permission.   Explain what happens when a malicious actor sends a large number of SYN packets all at once: When many SYN requests are sent to a destination, because of the protocols, the destination is obligated to process and answer to them; hence the server is overwhelmed by these requests, and cannot handle other eligible requests.  Explain what the logs indicate and how that affects the server: The logs indicate a single IP address, 203.0.113.0, attempts to perform a SYN flood attack to the server, and succeeds. |