# 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: the server has been overwhelmed with requests and cannot process them all.  The logs show that: There is an unusually high amount of SYN requests from one external IP address, which at first appears to connect properly, then later floods the server with even more SYN requests without completing the TCP protocol handshake, leading to all server requests even from legitimate employees to fail.  This event could be: a SYN attack, a form of a DOS 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. The first step is the SYN (synchronize) step. This is when the visitor requests to connect and receive information from the server. 2. Step 2 is the SYN, ACK (synchronize, acknowledge) step. This step confirms the server has received the request from the visitor and is ready to connect. 3. Step 3 is the ACK (acknowledge) step where the connection is confirmed.   Explain what happens when a malicious actor sends a large number of SYN packets all at once: When a malicious actor sends a large number of SYN packets all at once, the server will leave the same number of ports open so that the request can reach the 2nd and 3rd step of SYN-ACK and ACK. But a malicious actor in a SYN flood attack won’t complete the 2nd or 3rd step, therefore taking up all the ports from the server without completing it. This takes up all the bandwidth of the server, causing the server to crash if too many requests are sent.  Explain what the logs indicate and how that affects the server: The logs indicate that at first the SYN request from the malicious IP address (203.0.113.0) is accepted and completely as a normal visitor. But later the malicious attack from 203.0.113.0 sends many SYN requests without completing the TCP handshake steps 2 and 3. At first the employees are still able to connect as usual, but as the number of malicious SYN requests increases, soon all requests, even legitimate ones, are all met with error messages and the server can no longer keep up.  To secure the network in the future, it is recommended to block this IP address via a firewall. |