# Cybersecurity Incident Report

|  |
| --- |
| **Section 1: Identify the type of attack that may have caused this**  **network interruption** |
| The Network Protocol Analyzer indicates that, many employees cannot access to the company’s web server because of the quantity of SYN requests that the attacker is sending, SYN flooding, with the IP adress of 203.0.113.0. The web server is overwhelmed. |
|

|  |
| --- |
| **Section 2: Explain how the attack is causing the website to malfunction** |
| I received an automated alert from my monitoring system indicating a problem with the web server. You attempt to visit the company’s website, but you receive a connection timeout error message in your browser.  I used a packet sniffer to capture data packets in transit to and from the web server. I noticed many TCP SYN requests coming from an unfamiliar IP address. The web server appears to be overwhelmed by the volume of incoming traffic and is losing its ability to respond to the abnormally large number of SYN requests. I suspect the server is under attack by a malicious actor.  We should put the web server status as offline, to refresh and maybe block the attacker’s IP address in the firewall, knowing that it’s a temporary solution, because of IP Spoofing. |