# Cybersecurity Incident Report

|  |
| --- |
| **Section 1: Identify the type of attack that may have caused this**  **network interruption** |
| It is obvious that a singular traffic IP address (203.0.113.0) sent in a fury of SYN requests within a short time than normally seen in a healthy network. Similarly, this IP add was not a familiar one known to the organization's range of IP assignment. A flurry of SYN requests from a singular foreign IP within a short period without a corresponding SYN-ACK or ACK connections suggested a SYN Flood type of DOS attack. |
|

|  |
| --- |
| **Section 2: Explain how the attack is causing the website to malfunction** |
| Typical of a DOS attack, the malicious current of IP SYN requests came from a single IP address that was not know within the employees' assigned IP adds. Within 30s, we see over 100 SYN requests which overwhelmed the capacity of the web server to handle HTTPS requests. An overwhelmed web server cannot practically respond and complete the 3 ways handshake, including those of legitimate ones. DoS attacks renders an organization's service unreachable and ruins the reputation of the company. This kind of attack can be prevented in the future by increasing the capacity of servers to handle heavy traffic. In addition, the company can dynamically add IP addresses that violate request rate limits to restricted list. |