Cybersecurity Incident Report

|  |
| --- |
| **Section 1: Identify the type of attack that may have caused this**  **network interruption** |
| A device with the ip address of 203.0.113.0 appears to be creating a SYN flood attack by sending many SYN requests in a short period of time, creating a DoS attack. It appears this is a DoS attack, instead of a DDoS attack, since all requests are coming from 1 single ip address. . This appears to be a direct attack, since the ip address does not appear to be spoofing a legitimate device. |
|

|  |
| --- |
| **Section 2: Explain how the attack is causing the website to malfunction** |
| The server is being overloaded with SYN requests from a malicious actor which overwhelms the server's available resources to reserve for the connection. There are no server resource left for legitimate TCP connect requests. Since legitimate users can not access the website, it causes a negative impact on the organization because the users can not access the services/website they require. |