# Cybersecurity Incident Report

|  |
| --- |
| **Section 1: Identify the type of attack that may have caused this**  **network interruption** |
| **The attack that most likely caused this network interruption is known as an DoS SYN flood attack. The IP “203.0.113.0” is sending out a ton of SYN requests packets to the host IP. This in turn caused the issue that was experienced** |
|

|  |
| --- |
| **Section 2: Explain how the attack is causing the website to malfunction** |
| This attack is causing this website to malfunction because the attacker is sending out tons of SYN requests per millisecond. This is causing the website get overwhelmed by the amount of TCP handshake requests which “flood” the website causing it to be extremely slow or non-responsive at all. The attacker has successfully performed a DoS SYN flood attack which is resulting the web server to give out the error code 504. This means that the gateway has timed out due to the DoS attack. |