# Cybersecurity Incident Report

| **Section 1: Identify the type of attack that may have caused this network interruption** |
| --- |
| The attack seems to be arising from an IP 203.0.113.0.<br>The type of attack seems to be a SYN flood attack.<br>It is a Denial of service(DOS) attack as the SYN packets seems to be coming from the same IP in massive numbers, overwhelming the server. If it had been a distributed denial of service(DDOS) attack, the IP from which the SYN packets are being sent would have been different.<br>Because the server is overwhelmed by the number of packet it's getting which is causing the server to be unable to process with the real employees' requests as its busy answering to the attackers requests. |

| **Section 2: Explain how the attack is causing the website to malfunction** |
| --- |
| The attack is a denial of service(DOS) attack. It is identified when several requests are received from the same IP within a second.<br>This attack has stopped the normal functioning of the organization's website. Employees are not being able to go to the requested site and getting errors.<br>If this goes on the employees will not be able to visit the company's site and perform their daily task. This may also monetarily harm the company if not fixed immediately.<br>This type of attack can be prevented in future by installing a firewall and adding a rule to not accept too many requests from one IP. Alternatively, an IPS can also be installed. |