# Cybersecurity Incident Report

|  |
| --- |
| **Section 1: Identify the type of attack that may have caused this**  **network interruption** |
| That would be the DOS attack by flooding the server with SYN packets. And it’s a DOS attack because only 1 IP address is used for the attack which is 203.0.113.0. |
|

|  |
| --- |
| **Section 2: Explain how the attack is causing the website to malfunction** |
| The attack pattern is clear enough that it’s a DOS attack, as we can see in the sequence of events that multiple legitimate users established a TCP connection and got the HTML page from the website performing the handshake procedure successfully, but after persistent interruptions from source 203.0.113.0, the server couldn’t fulfill requests for other users and eventually ran out of resources due to the flooding of SYN packets by the attacker IP, which then leads to actual users not being able to access the service, which has the potential to cause financial damages, reputational damages and more damages including even medical damages if the service is medical in its nature.  Perhaps a proper way to stop this attack would be banning the IP address, but that only stops the attack from that source, alternatively I would recommend if such an option is available, that a firewall rule be implemented so that when an source IP only tries to send SYN packets a maximum number of times, it’d place them on a timeout from the server and then trigger a function to copy the attempts of that IP(s) and dump them in a log to be investigated further for a potential ban by an analyst. |