# Cybersecurity Incident Report:

# Network Traffic Analysis

|  |
| --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log |
| The network protocol analyzer logs indicate that there have been suspicious number of SYN requests under the TCP Protocol from the same Source IP address 203.0.113.0 to the Destination IP 192.0.2.1. It is very possible that this is an indication of a malicious attack. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide one solution to implement |
| When attempting to visit the company’s website, a connection timeout error message is shown on the browser. To investigate the issue, we conducted a packet sniffing tests using tcpdump. In the resulting logs, we found that the first SYN request from Source IP address 203.0.113.0 was sent to the Destination IP 192.0.2.1 according to log number 52. Even though the Destination IP returned [SYN, ACK] and the Source IP returned [ACK], after 0.22 seconds in log 57, the same Source made SYN request to the Destination IP. Looking at logs from 125 to 214, every log is a SYN request from 203.0.113.0 to the Destination IP. Since this may be a DOS attack, our team will proceed with the company’s playbook to shutdown the server to defend against further attacks. We are in process of adding additional web application firewalls, secure web gateways, and other DOS protection technologies to protect the assets so our clients can access our website safely. |