# 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 is giving an error message that says “ port 53 is unreachable” but in the log i can see that the message comes from the same ip address two more times. ICMP error messages should only be sent once per request. This raises my concerns of a Dos attack . | |
|

| Part 2: Explain your analysis of the data and provide one solution to implement |
| --- |
| I was made aware of this issue when i received multiple calls from customers that they could not access the website. So i responded by trying to access the website myself and i wasnt able to either. I then set up my network protocol analyzer and thats when i got the error messages that i mentioned above. Since this has to do with the internet layer of network protocols . The next steps that the team and i will take is determining if the DNS server is down or if traffic to port 53 is being blocked by a firewall. We can also try getting in contact with the company to see if they are experiencing network issues. If they confirm that they are we will begin Implementing our playbooks for ICMP flooding attacks. |