# Cybersecurity Incident Report:

# Network Traffic Analysis

|  |
| --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log |
| The network analysis log shows that Port 53 is unreachable at destination website, when trying to send over ICMP packet. Port 53 is seen unreachable in 3 instances meaning there could be a malicious attack happening at destinations Ip: 192.51.100.15. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide one solution to implement |
| Error was reported this afternoon at 1300 hours as we started the investigation using the network protocol analyzer tool tcpdump. Which showed that port 53 is unreachable using the HTTPS protocol. The root cause of this failure is unknown, but the network team is currently working to fix this issue. But the team that disclosed this issue believes the cause could possibly be a (DDOS) attack coming from a disgruntle employee. When looking at the TCPDUMP there is evidence that the attack is coming from an internal network IP address: 203.0.113.2, further investigation is required. |