# Cybersecurity Incident Report:

# Network Traffic Analysis

| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log. | |
| --- | --- |
| The UDP protocol reveals that:  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message:  The port noted in the error message is used for:  The most likely issue is: | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| Time incident occurred: 1:24 p.m., 32.192571  Explain how the IT team became aware of the incident: the website page was not loading and had a message saying that the port 53 is not accessible  Explain the actions taken by the IT department to investigate the incident: IT departement tried loading the website and got the error message then we used the tcpdump to analyze the packets.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): the Port affected is port 53 which a port used by DNS and the protocol used is UDP  Note a likely cause of the incident: a Likely cause is a dos or ddos attack on the dns server which caused to go down |