# 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:UDP packet was undeliverable Port 53 .  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: UDP port 53 unreachable.  The port noted in the error message is used for: DNS service  The most likely issue is:Denial of service(DOS) Attack. | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| Time incident occurred: 1:24 pm  Explain how the IT team became aware of the incident:several customers reported that they were unable to access the company website and saw the error message saying the destination port is unreachable after trying to log in the website.  Explain the actions taken by the IT department to investigate the incident: they load their network analyzer tool, tcpdump, and attempt to load the webpage again. To load the webpage, their browser sends a query to a DNS server via the UDP protocol to retrieve the IP address for the website's domain name.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): port 53 is affected which is the port for dns service  Note a likely cause of the incident:This looks like a denial of service (dos) attack attempting to disrupt normal business operation by overloading the network. |