# 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: DNS server was unreachable as network protocol analyzer indicates that port 53 is unreachable  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: UDP port 53 is unreachable  The port noted in the error message is used for: Domain Name Server (DNS)  The most likely issue is: maybe a firewall misconfiguration as the message didn't go through to DNS server | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| Time incident occurred: The incident occurred at afternoon at lunch time  Explain how the IT team became aware of the incident:Several customers contacted our company to report that they were not able to access the company website www.yummyrecipesforme.com, and saw the error “destination port unreachable” after waiting for the page to load.  Explain the actions taken by the IT department to investigate the incident: we have tried to replicate the issue once replicated used tcpdump to analyze the network traffic  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): through tcpdump was able to find that UDP port 53 is unreachable which commonly used for DNS  Note a likely cause of the incident: Firewall misconfiguration or can be a DOS attack |