# 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: It reveals that one of the ports 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 unreachable  The port noted in the error message is used for: It is the port for the DNS servers which translates domain names into IP addresses.  The most likely issue is a denial-of-service attack to the DNS server from a threat actor. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred: 13:24:32:192571 [=] 1: 24 pm  Explain how the IT team became aware of the incident: They became aware of the incident due to several customers contacting them about their inability to access the yummy website.  Explain the actions taken by the IT department to investigate the incident: They used the tcpdump network analyzer tool to attempt to load the webpage in order to analyze the data traffic within the network  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): That the DNS service port 53 was unreachable  Note a likely cause of the incident: The likely cause could be a denial of service (DOS) attack, ICMP flood attack or issue with the port configuration. |