# 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:  The DNS protocol used UDP to contact the DNS server and retrieve the IP address for the domain name yummyrecipesforme.com. However, the ICMP protocol returned an error message, indicating a problem reaching the DNS server. The first two lines of each log event show the UDP request from your browser, while the third and fourth lines display the ICMP error, stating “udp port 53 unreachable.” Since port 53 is for DNS traffic, this suggests a DNS server issue. The presence of flags in the UDP message and the "A?" symbol further indicates problems with the DNS protocol. The ICMP error suggests the DNS server is likely unresponsive. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred:  Explain how the IT team became aware of the incident:  Explain the actions taken by the IT department to investigate the incident:  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):  Note a likely cause of the incident:  The incident occurred today at 1:24 p.m. Customers reported receiving a “destination port unreachable” message when trying to visit yummyrecipesforme.com. The cybersecurity team is currently investigating to restore website access. Packet sniffing tests using `tcpdump` revealed that DNS port 53 is unreachable. The next step is to determine if the DNS server is down or if traffic to port 53 is being blocked by a firewall, possibly due to a Denial of Service attack or a misconfiguration. |