# Cybersecurity Incident Report:

# Network Traffic Analysis

|  |
| --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log. |
| In a network analysis, UDP protocol encountered issues, failing to access the desired protocol or deliver to the DNS server's port. This became evident when an ICMP echo reply resulted in an error message. The port specified in the error message is typically used for managing communications. The root problem appears to be the use of the UDP protocol for requesting domain name resolution via the DNS server's address on port 53. This mismatch likely led to the reported issues in network communication. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| At 13:24:32.192571, an incident arose when several customers reported their inability to access the company website, www.yummyrecipesforme.com. In response, the IT department-initiated investigations, starting by verifying the issue on the website itself and later utilizing a network analyzer tool, which revealed a substantial packet influx.  During their analysis, the IT team uncovered crucial details, particularly regarding the affected port and the DNS server. The network analyzer displayed an error message: "udp port 53 unreachable." This finding pointed to the use of UDP protocol for requesting domain name resolution via the DNS server's address on port 53, which is conventionally associated with DNS services.  The term "unreachable" within the error message indicated that the message failed to reach the DNS server. This essentially implied that there was no service actively listening on the designated DNS port. Consequently, browsers were unable to retrieve the IP address necessary to access yummyrecipesforme.com, leading to the reported accessibility issue on the website. |