# Cybersecurity Incident Report: Network Traffic Analysis

A screenshot of a computer program

Description automatically generated

# 

|  |
| --- |
| Part 1: Provide a summary of the problem found in the tcpdump log |
| The analysis of the DNS and ICMP traffic log indicates that the incident revolves around a DNS resolution request sent via the UDP protocol. As part of the DNS protocol, the UDP protocol was used to contact the DNS server to retrieve the IP address for the domain name of yummyrecipesforme.com. The ICMP protocol was used to respond with an error message, indicating issues contacting the DNS server. The UDP message going from your browser to the DNS server is shown in the first two lines of every log event. The ICMP error response from the DNS server to your browser is displayed in the third and fourth lines of every log event with the error message, “udp port 53 unreachable.” Since port 53 is associated with DNS protocol traffic, we know this is an issue with the DNS server. This ICMP error message suggests that the DNS resolution request failed to reach the DNS server over the specified port, thus preventing the retrieval of the necessary IP address. The most likely cause of this issue is a configuration problem or blockage affecting the flow of traffic to UDP port 53, possibly due to firewall rules or network settings. |
|  |

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| The incident occurred today at 1:24 p.m. Customers notified the organization that they received the message “destination port unreachable” when they attempted to visit the website yummyrecipesforme.com. The cybersecurity team providing IT services to their client organization are currently investigating the issue so customers can access the website again. In our investigation into the issue, we conducted packet sniffing tests using tcpdump. The ICMP error message consistently indicated that UDP port 53, integral for DNS service, was inaccessible. The next step is to identify whether the DNS server is down or traffic to port 53 is blocked by the firewall. The DNS server might be down due to a successful Denial of Service attack or a misconfiguration. |