# Cybersecurity Incident Report: Network Traffic Analysis

|  |
| --- |
| Part 1: Provide a summary of the problem found in the tcpdump log |
| In the context of the DNS protocol, the UDP protocol is utilized to reach the DNS server in order to obtain the IP address for the domain name yummyrecipesforme.com. An ICMP protocol was employed to send back an error message indicating problems in contacting the DNS server. The first two lines of each log event display the UDP message from your browser to the DNS server. The third and fourth lines show the ICMP error response from the DNS server to your browser, accompanied by the error message “udp port 53 unreachable.” Given that port 53 is designated for DNS protocol traffic, this points to an issue with the DNS server. Additional indications of problems with the DNS protocol are apparent, as the plus sign following the query identification number 35084 signifies flags associated with the UDP message, while the “A?” symbol reflects the flags related to DNS operation requests. The ICMP error response regarding port 53 strongly suggests that the DNS server is unresponsive. This conclusion is further bolstered by the flags linked to the outbound UDP message and the domain name resolution attempt. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| The incident took place today at 1:24 p.m. Customers reported to the organization that they encountered the message "destination port unreachable" when trying to access the website yummyrecipesforme.com. The cybersecurity team responsible for providing IT support to the client organization is currently investigating the matter to restore customer access to the site. During our investigation, we performed packet sniffing tests using tcpdump. The resulting log file indicated that DNS port 53 was unreachable. Our next step is to determine whether the DNS server is down or if traffic to port 53 is being blocked by the firewall. The unavailability of the DNS server could be due to a successful Denial of Service attack or a configuration error. |

