# Cybersecurity Incident Report:

# Network Traffic Analysis

|  |
| --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic 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. This request is crucial for translating the website's domain name into an IP address. However, the response from the DNS server indicates that the UDP port 53, a well-known port for DNS service, is unreachable. 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 came to the attention of the IT team through reports from customers who were unable to access the website www.yummyrecipesforme.com. In response, the IT department employed a network analyzer tool, tcpdump, to capture packets during a website access attempt. This analysis uncovered a recurring pattern: the DNS resolution request, transmitted via UDP, encountered an unreachable destination port issue. The ICMP error message consistently indicated that UDP port 53, integral for DNS service, was inaccessible. Given these findings, a probable cause of the incident appears to be a hindrance in communication due to a potential misconfiguration or blockage that is preventing the DNS resolution request from reaching the DNS server via UDP port 53. To address this, the IT department plans to collaborate with security engineers for further investigation into the network configuration, firewall settings, and potential solutions to resolve this accessibility concern. |