# Cybersecurity Incident Report:

# Network Traffic Analysis

|  |
| --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log |
| The network protocol analyzer logs indicate that port 53 is unreachable when attempting to reach the website [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com). Port 53 is used for TCP/UDP traffic to access the DNS servers, which translate a query for a website name into an IP address so that the web server can create a connection to the client. This issue may be caused by a problem with the DNS server itself, firewall configurations, or potentially issues that are occurring during the TCP handshake. IT is also possible that malicious attackers are targeting the DNS server as well. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide one solution to implement |
| This incident occurred at 1:24 pm today, and was reported by customers attempting to reach the yummyrecipesforme website. When trying to access the website, the website would not load and received the message “destination port unavailable.”  I used the network protocol analyzer tool, tcpdump, to check to connection. I received ICMP response that UDP port 53 (used by DNS protocol) is unreachable. Our next steps are to check the firewall configuration to see if port 53 has been blocked, as well as contacting the system administrator for the web servers to check the systems for signs of a potential DoS attack. |