# Cybersecurity Incident Report:

# Network Traffic Analysis

| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log | |
| --- | --- |
| The tcpdump network protocol analyzer logs indicate that port 53 is unreachable when attempting to access the Yummysrecipesforme website. I sent an ICMP request packet and got an error message saying it was undeliverable to the port of the DNS server. Using the UDP protocol as well, to request a domain name resolution using the address of the DNS server over port 53 stated it was unreachable as well. Which in turn we weren't able to get the IP address for the website which we needed as no service was listening on the receiving DNS port as indicated by the ICMP error message “UDP port 53 unreachable.” This may indicate a problem on the internet layer of the system according to the TCP/IP model and the web server itself or a compromised firewall. | |
|

| Part 2: Explain your analysis of the data and provide one solution to implement |
| --- |
| We realized the extent of this problem when we received calls from clients indicating it was affecting them as well and they all told us they got the error message “destination port unreachable” when trying to use our website. We later found that the incident started at 1:23pm. We are actively working diligently to resolve this issue so that our website will be accessible again to everyone. To investigate this issue, we issued a packet sniffer analyzer tool called tcpdump to give us a breakdown of the specific errors that occurred and where. In turn, we found that DNS port 53 was unreachable. The cause of this could either be our firewall blocking our entrance for containment purposes or that the DNS server might be down due to a successful Denial of Service attack or it could be a misconfiguration. Regardless we will work tirelessly to get the website back up and running as soon as possible. |