# Cybersecurity Incident Report:

# Network Traffic Analysis

|  |
| --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log. |
| The UDP protocol reveals that “udp port 53” is unreachable, The port 53 is normally used for DNS services, the word “unreachable” indicated that the UDP message tried to request for an IP Address for the domain of “www.yummyrecipesforme.com” and it did not go through the DNS server`, the issue is most likely is that no one is listening one the receiving DNS port. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| It was around 1:24 PM and our customers reported that they could not access the website “www.yummyrecipesforme.com”, their reports included that they saw an error “destination port unreachable” after trying to access the website which indicates a legitimate error, the IT team made an attempt to visit the website and to no avail the same error still exists on our end, next we used a network analyzer tool, tcpdump and attempt to load the webpage again, the analyzer receives ICMP packets which came from sending UDP packets to the DNS server, the ICMP packet read “udp port 53 unreachable”. In lay man’s term to load a webpage your browser requests a query to a DNS server via the UDP protocol to retrieve an IP Address for a website domain name, this is called a DNS protocol, the likely cause for all of this is either the port 53 is accidentally port filtered (misconfigured) by accident or a DoS (Denial of Service) attack has occurred. |