# 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: UPD was used to make contact with DNS in order to get the IP address that corresponds to the website domain. Then, ICMP was used to tell about a transmission error trying to request DNS, such as the port 53 is unreachable when attempting to access the client company website.  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: ICMP 203.0.113.2 udp port 53 unreachable.  The port noted in the error message is used for: port 53 DNS protocol traffic service.  The most likely issue is: the main issue is with the DNS server. We think it’s probably the fact that the DNS server isn’t responding at all. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred: 13:24 or 1:24 pm  Explain how the IT team became aware of the incident: several customers of clients reported that they were not able to access the client company website [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com) and saw the error “destination port unreachable” after waiting for the page to load.  Explain the actions taken by the IT department to investigate the incident: attempted to visit the website, we received ICMP error, load tcpdump packet sniffer to enter the webpage, send a query to DNS server via UPD protocol to retrieve the IP address for the websites domain name. Use the IP address for sending HTTPS request to display the webpage. Analyze tcpdump log.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): udp port 53 which is used for DNS protocol traffic its unreachable because the DNS does not respond.  Note a likely cause of the incident: the DNS server isn’t working as a result of a possible denial of service attack (DoS) which caused and overload on the DNS and that’s why isn’t able to respond. |