

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 the DNS server is unreachable when attempting to access the website with the domain name; yummyreceipesforme.com  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: "UDP port 53 unreachable"  The port noted in the error message is used for sending DNS query to the DNS server to retrieve the IP address of the website.  The most likely issue is that the DNS server may be unavailable or there is a firewall on the DNS server blocking UDP traffic on port 53. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| The incident occured at about 1:24 p.m in the afternoon.  Clients reported that they were not able to access the yummyreceipesforme.com website and saw the error "destination port unreachable" after waiting for the page to load  In the investigation done by the IT department, we first loaded our network analyser tool, tcpdump and attempted to load the webpage again by sending a query to the DNS server via the UDP protocol to retrieve the IP address for the website's domain name.  Our browser then used this IP address as the destination IP address for sending an HTTPS request to view the webpage  Our investigation showed that when we sent UDP packets to the DNS server, we received ICMP packets containing the error message "udp port 53 unreachable"  The likely cause of the incident could be that the DNS server is unavailable or there is a firewall configuration on the DNS server blocking UDP traffic. |