# 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.  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: The standard port for DNS is port 53. DNS client applications use the DNS protocol to query and request information from DNS servers, and the server returns the results to the client using the same port. Port 53 is used for both TCP and UDP communication.  The most likely issue is: The message did not go through to the DNS server. The browser was not able to obtain the IP address for yummyrecipesforme.com, which it needs to access the website because no service was listening on the receiving DNS port as indicated by the ICMP error message “udp port 53 unreachable.” |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred: the timestamps indicate that the event happened at 1:24 p.m., 32.192571 seconds. For example: 13:24:32.192571  Explain how the IT team became aware of the incident: Several customers contacted your company to report that they were not able to access the company website 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: To start, the team visited the website and they also received the error “destination port unreachable.” Next, the team loaded the analyzer tool, tcpdump, and load the webpage again. This time, they received lot of packets in network analyzer. The analyzer shows that when they send UDP packets and receive an ICMP response returned to their host, the results contain an error message: “udp port 53 unreachable.”  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):  Timestamps: 13:24:32.192571. This displays the time 1:24 p.m., 32.192571 seconds.  The source and destination IP address: 192.51.100.15.52444 > 203.0.113.2.domain . To the left is source and to the right side is the destination address.  Response from ICMP request packet: “udp port 53 unreachable”  Note a likely cause of the incident: The word “unreachable” in the message indicates the message did not go through to the DNS server. Your browser was not able to obtain the IP address for yummyrecipesforme.com, which it needs to access the website because no service was listening on the receiving DNS port as indicated by the ICMP error message “udp port 53 unreachable.” |

This activity was also done using Wireshark

A screenshot of a computer program

Description automatically generated