# 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: There is no response from the DNS server when trying to access the desired website.  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: udp port 53. Port 53 seems to be a port for DNS service. The word "unreachable" in the message indicates the UDP message requesting an IP address for the domain "www.yummyrecipesforme.com" did not go through to the DNS server because no service was listening on the receiving DNS port.  The port noted in the error message is used for: Port 53 is used for Domain Name System (DNS) communication, both TCP and UDP,  The most likely issue is: Seems most likely an issue with the DNS server due to no response from its side. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred: 13:24:32  Explain how the IT team became aware of the incident: Due to clients’ reports about the website not being accessible.  Explain the actions taken by the IT department to investigate the incident: First the website was tried to be accessed via browser, getting a “destination port unreachable” as response, then a deep analysis with tcpdump was performed to check any ICMP erros when reaching the website  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): The website [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com), can not be accessed, as the DNS port (53) seems to be down as there was not response from the DNS server when doing a request for the website IP address’.  Note a likely cause of the incident: Seems to be a DOS attack on the DNS server. |

Snapshot from the packet sniffing analysis

A white text with black numbers

AI-generated content may be incorrect.