# 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 repeated DNS queries suggest that the source is attempting to resolve the domain "yummyrecipesforme.com" at different timestamps.  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: The ICMP messages indicate that the destination server (203.0.113.2) is unreachable on UDP port 53  The port noted in the error message is used for: Port 53 is Commonly used for DNS  The most likely issue is:   1. The destination DNS server might be down or unreachable. 2. There could be a network issue preventing communication between the source and destination. 3. A firewall or security device may be blocking the communication. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred: 13.24.32, 13.26.32 and 13.28:32  Explain how the IT team became aware of the incident:  Several customers reported the issue and brought the attention to IT.  Explain the actions taken by the IT department to investigate the incident:   1. **Customer Reports Analysis:** The IT team likely started by collecting and analyzing customer reports to understand the nature and scope of the issue. This involved gathering information on error messages, affected users, and the specific symptoms reported. 2. **Initial Troubleshooting:** The IT team may have performed initial troubleshooting steps, such as checking the server status, reviewing server logs, and attempting to access the website from different locations to reproduce the issue. 3. **Network Traffic Analysis:** Since the issue involved a "destination port unreachable" error, the IT team used network analyzer tools, such as tcpdump, to capture and analyze network traffic related to the problematic domain ([www.yummyrecipesforme.com](http://www.yummyrecipesforme.com)).   Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):   * **Affected Protocol:** The issue is related to the UDP protocol, specifically UDP packets sent to the DNS server (port 53). * **Error Message:** The ICMP packets received in response to UDP packets contain the error message "udp port 53 unreachable."   Note a likely cause of the incident:   **Verify DNS Server Status:** Confirm the status and availability of the DNS server that handles requests for [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com) (potentially located at 203.0.113.2). Check for any issues, outages, or misconfigurations.   **Network Reachability:** Investigate the network path between the source (192.51.100.15) and the DNS server (203.0.113.2). Ensure that there are no network issues, such as firewalls blocking communication. |