# Cybersecurity Incident Report:

# Network Traffic Analysis

| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log. | |
| --- | --- |
| The DNS and ICMP traffic log shows that the website [*www.yummyrecipesforme.com*](http://www.yummyrecipesforme.com/) is inaccessible due to the destination port being unreachable. The log reveals that the DNS query was sent using the UDP protocol, but the response was an ICMP message indicating that UDP port 53 was unreachable. This ICMP error was returned three times, consistently indicating the same issue. As a result, the DNS resolution fails, preventing access to the website. | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| **Time Incident Occurred:**  Based on the provided timestamps in the tcpdump log, the incident occurred around 13:24 PM (1:24 PM).  **How IT Team Became Aware of the Incident:**  The IT team likely became aware of the incident through multiple channels:   1. User Reports: Multiple customers reported difficulties accessing the website and received the "destination port unreachable" error. 2. Monitoring Tools: Network monitoring tools might have detected anomalies in DNS traffic or website accessibility. 3. Internal Testing: IT staff might have attempted to access the website themselves and encountered the same issue.   **Actions Taken by the IT Department to Investigate the Incident:**   1. Network Analysis: The IT team utilized a network analyzer tool like tcpdump to capture network traffic and analyze the issue. 2. DNS Server Check: The team would have checked the status and configuration of the DNS server, including its logs. 3. Firewall Inspection: The firewall rules were likely reviewed to ensure that DNS traffic was not being blocked. 4. Network Connectivity Verification: The team would have verified network connectivity between the website server and the DNS server.   **Key Findings of the IT Department's Investigation:**   * Affected Port: The incident primarily affected UDP port 53, which is the standard port for DNS services. * DNS Server Issue: The DNS server was not responding to DNS queries, leading to the "destination port unreachable" error.   **Likely Cause of the Incident:**  A likely cause of the incident could be a DNS server malfunction or outage. This could be due to various factors, such as:   * Hardware failure: A hardware component of the DNS server might have failed. * Software bug: A software bug in the DNS server software could have caused it to malfunction or crash. * Overload: The DNS server might have been overloaded with too many requests, leading to performance degradation or complete failure. * Network connectivity issues: Problems with the network connectivity between the website server and the DNS server could have prevented DNS queries from reaching the server.   By analyzing the network traffic and investigating the DNS server, the IT team can pinpoint the exact cause of the incident and take appropriate corrective actions to restore normal website access. |