# 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:** UDP packets were sent from the client's computer (IP: 192.51.100.15) to the DNS server (IP: 203.0.113.2) on port 53 to request the IP address for the domain [www.yummyrecipesforme.com](http://www.yummyrecipesforme.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." This indicates that the DNS server was not accepting UDP packets on port 53, which is the standard port for DNS queries.  **The port noted in the error message is used for:** Port 53, which is used for DNS (Domain Name System) services. DNS is essential for translating domain names into IP addresses, allowing users to access websites using human-readable addresses.  **The most likely issue is:** The DNS service on the server at IP address 203.0.113.2 is either down or not properly configured to listen on UDP port 53. This could be due to a misconfiguration, the DNS service being stopped, or a firewall or network policy blocking UDP traffic on port 53. | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| **Time Incident Occurred:** The incident occurred at 13:24:32, based on the timestamp of the first UDP packet sent to the DNS server.  **Explanation of How the IT Team Became Aware of the Incident:** The IT team became aware of the incident when several customers reported being unable to access the website [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com) and seeing the error "destination port unreachable." An attempt by an internal user to access the website confirmed the issue.  **Actions Taken by the IT Department to Investigate the Incident:**   1. **Initial User Report Verification:**    * An internal attempt to access the website was made, resulting in the same "destination port unreachable" error. 2. **Network Analysis Using tcpdump:**    * The IT team used tcpdump to capture and analyze network traffic between the client computer and the DNS server.    * The captured log data was examined to identify the source and nature of the issue.   **Key Findings of the IT Department's Investigation:**   1. **Outgoing UDP Requests:**    * The client computer (IP: 192.51.100.15) sent UDP packets to the DNS server (IP: 203.0.113.2) on port 53, requesting the IP address for the domain [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com). 2. **ICMP Responses:**    * The DNS server (IP: 203.0.113.2) responded with ICMP error messages indicating "udp port 53 unreachable."    * This error was consistent across multiple attempts, suggesting a persistent issue with UDP port 53 on the DNS server.   **Likely Cause of the Incident:** The DNS service on the server at IP address 203.0.113.2 is either not running or not properly configured to listen on UDP port 53. Potential causes include:   * **DNS Service Configuration Issue:** The DNS service may be misconfigured, preventing it from listening on port 53. * **DNS Service Down:** The DNS service might be stopped or crashed. * **Firewall or Network Policy:** A firewall or network policy may be blocking UDP traffic on port 53. * **Recent Changes or Updates:** Any recent changes or updates to the DNS server configuration could have inadvertently affected its operation. |

**Conclusion and Recommendation:** To resolve the issue, the IT team should:

1. Verify the configuration and status of the DNS service on the server at 203.0.113.2.
2. Check firewall and network policies to ensure that UDP traffic on port 53 is permitted.
3. Restart the DNS service and monitor its performance.
4. Investigate any recent changes or updates that might have impacted the DNS server's configuration.