# 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 UDP protocol is being used for DNS queries from the client (192.51.100.15) to the DNS server (203.0.113.2). However, the DNS server is not responding to these queries, and instead, ICMP error messages are being returned.  **This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message:**  The ICMP error messages indicate that the UDP port 53 is unreachable. The specific error message is "ICMP 203.0.113.2 udp port 53 unreachable."  **The port noted in the error message is used for:**  Port 53 is the standard port used for DNS (Domain Name System) queries and responses. It is essential for resolving domain names to IP addresses.  **The most likely issue is:**  The most likely issue is that the DNS server at 203.0.113.2 is either down, misconfigured, or experiencing network connectivity issues, preventing it from responding to DNS queries 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 was first observed at **13:24:32.192571** and continued to occur in subsequent log entries at **13:26:32.192571** and **13:28:32.192571**.  **Explain how the IT team became aware of the incident:**  The IT team became aware of the incident through network monitoring tools that detected repeated DNS query failures and ICMP error messages in the network traffic logs.  **Explain the actions taken by the IT department to investigate the incident:**  The IT department reviewed the tcpdump logs to identify patterns in the DNS queries and ICMP error messages. They focused on the DNS server's status, configuration, and network connectivity to determine the root cause of the issue.  **Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):**   * The DNS server at 203.0.113.2 is not responding to UDP requests on port 53. * ICMP error messages consistently indicate that port 53 is unreachable. * The client (192.51.100.15) repeatedly attempts to query the DNS server for the domain "yummyrecipesforme.com," but the server fails to respond.   **A likely cause of the incident:**  The likely cause of the incident is that the DNS server is under a **DDoS (Distributed Denial of Service) attack**. The attack is overwhelming the server's resources, causing it to become unresponsive to legitimate DNS queries. This results in ICMP "port unreachable" errors and repeated DNS query attempts from the client. |