# Cybersecurity Incident Report:

# Network Traffic Analysis

|  |
| --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log. |
| The network analyzer log indicates repeated DNS queries over UDP sent from the client IP (192.51.100.15) to the DNS server IP (203.0.113.2) on port 53, which is standard for DNS services. This analysis shows that the ICMP echo reply returned the error message "udp port 53 unreachable." This indicates that the DNS server at 203.0.113.2 is not responding to the DNS queries sent to it. Port 53 is used for DNS services to handle requests and responses for resolving domain names to IP addresses. The most likely issue is that the DNS server at 203.0.113.2 is either down, not configured to listen on port 53, or there is a network/firewall issue blocking UDP traffic to port 53. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| The incident was first recorded at 13:24:32 (1:24 p.m.), based on the timestamps in the tcpdump log. The IT team became aware of the incident after several customers reported that they could not access the client company website, www.yummyrecipesforme.com, and were receiving the error "destination port unreachable." The IT team then attempted to access the website and confirmed the same error message. To investigate, the IT department ran a network protocol analyzer tool, tcpdump, while attempting to load the webpage again. They captured the network traffic between the client and the DNS server to identify the issue.  Key findings of the IT department's investigation revealed that DNS queries were sent from the client IP (192.51.100.15) to the DNS server IP (203.0.113.2) on port 53 using UDP. The DNS server responded with ICMP error messages indicating "udp port 53 unreachable." This error indicates that the DNS server is either not running or there is a network configuration issue preventing DNS queries from being processed. The most likely cause of the incident is that the DNS server at IP 203.0.113.2 is not properly configured to handle DNS queries on port 53, or there is a firewall or network issue blocking UDP traffic to this port. |