# Cybersecurity Incident Report:

# Network Traffic Analysis

|  |
| --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log. |
| The tcpdump logs show that the initial outgoing request from your computer to the DNS server was attempting to resolve the domain "yummyrecipesforme.com" using the UDP protocol. The DNS query was sent to port 53 of the DNS server with the source IP address being your computer's IP address (192.51.100.15) and the destination IP address being the DNS server's IP address (203.0.113.2). The query was flagged as a DNS request for an A record, which is used to map the domain name to an IP address.  However, the server responded with an ICMP "Destination Unreachable" error, specifically indicating that the UDP packet was undeliverable to port 53. The error message, "udp port 53 unreachable," suggests that the DNS server was not accepting the request, either due to a configuration issue or an unavailable service on the DNS server at the time.  The error occurred multiple times, as the log indicates that ICMP packets were sent twice more, but each resulted in the same error response. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| The incident occurred at 13:24:32.192571 (1:24 PM and 32.192571 seconds) when an attempt to resolve the domain "yummyrecipesforme.com" failed. The IT team became aware of the issue when users were unable to access the website, prompting an analysis of the network traffic.  Upon reviewing the tcpdump log, it was found that the DNS query was being sent from the internal machine with the IP address 192.51.100.15 to the DNS server at 203.0.113.2. The expected response from the DNS server, however, was an ICMP error message indicating that UDP port 53, the port used for DNS queries, was unreachable. This could indicate that either the DNS server was down, or there was an issue with the configuration of the server or the firewall that is blocking the DNS traffic.  The key findings in the analysis were:   * Source IP: 192.51.100.15 (your computer) * Destination IP: 203.0.113.2 (DNS server) * Protocol: UDP, for DNS query (A record lookup) * ICMP Error: "Destination Unreachable" – "udp port 53 unreachable" * The DNS query failed to reach the server due to the server not responding on the expected DNS port (53).   The most likely cause of the incident is that the DNS server was either down, or a firewall or misconfiguration was blocking UDP traffic to port 53, preventing the DNS query from being resolved. Further investigation into the DNS server's status or configuration changes may be necessary to resolve the issue. |