# 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: DNS queries were sent from 192.51.100.15 to the domain yummyrecipesforme.com on port 53. However, multiple ICMP error messages indicate that the DNS server 203.0.113.2 is unreachable. This suggests a potential issue with DNS resolution or the network path to the DNS server.  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: "Destination Port Unreachable".  The port noted in the error message is used for: DNS (Domain Name System), which operates on UDP port 53.  The most likely issue is: Either the DNS server 203.0.113.2 is down, misconfigured, or there is a network routing issue preventing communication between the source (192.51.100.15) and the DNS server. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred: The incident was logged at multiple timestamps:  13:24:32  13:26:32  13:28:32  Explain how the IT team became aware of the incident: Repeated ICMP "Destination Port Unreachable" messages were observed in the network traffic logs, indicating failed DNS queries.  Explain the actions taken by the IT department to investigate the incident: Reviewed network traffic logs for anomalies.  Checked the availability and configuration of the DNS server 203.0.113.2.  Verified the network connectivity between the source device (192.51.100.15) and the DNS server.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): The affected port is UDP port 53, used for DNS queries.  The DNS server 203.0.113.2 is unreachable.  The source device 192.51.100.15 repeatedly attempted to resolve the domain yummyrecipesforme.com.  Note a likely cause of the incident: The DNS server 203.0.113.2 could be offline or misconfigured, or there might be a network path issue (e.g., firewall blocking, routing problems) preventing successful DNS resolution. |