# Cybersecurity Incident Report:

# Network Traffic Analysis

|  |
| --- |
| Part 1: Provide a summary of the problem(s) found in the DNS and ICMP  traffic log. |
| The UDP protocol reveals that:  **13:24:36.098564 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2 UDP port 53 unreachable length 254**   * **As the Host device tried to access the DNS Server it got an error message stating that port 53 was unreachable.**   This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message:  **“ICMP 203.0.113.2 UDP port 53 is unreachable”.**   * **The TCPDIMP output showed repeated ICMP Destination Unreachable messages for UDP port 53, confirming that DNS queries were not reaching a listening service.**   The port noted in the error message is used for:  **The port noted in the error message is used for DNS (Domain Name Service).**  The most likely issue is:  **The most likely issue is the UDP message requesting an IP address for the domain** [**www.yummyrecipesforme.com**](http://www.yummyrecipesforme.com) **did not go through to the DNS server because no service was listening on the receiving DNS port.** |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred:  **First Analysis: The incident began at 13:24:32.192571 – 13:24:36.098564:**  **which translates to:**  **1:24PM 32 Seconds & 192571 milliseconds - 1:24PM 36 Seconds & 098564 milliseconds**  **Second Analysis: Incident began at 13:26:32.192571 – 13:27:15.934126:**  **Which translates to:**  **1:26PM 32 Seconds & 192571 Milliseconds – 1:27PM 15 Seconds & 934126 Milliseconds.**  **Third Analysis: The Incident began at 13:28:32.192571 – 13:28:50.022967:**  **Which translates to:**  **1:28PM 32 Seconds & 192571 Milliseconds – 1:28PM 50 Seconds & 022967 Milliseconds.**  **These all took place in the Afternoon.**  Explain how the IT team became aware of the incident:  **The IT team became aware of the incident by analyzing the situation and determining which network protocol was affected during this incident. First there was an attempt to visit the website and there was an error “destination port unreachable”.**  Explain the actions taken by the IT department to investigate the incident:  **To investigate the IT department troubleshooted the issue, with the network analyzer tool (TCPDUMP) and attempts to load the page again were executed. The Analyzer showed that when the UDP packets were sent to the DNS server, ICMP packets were received containing the error message “UDP port 53 unreachable”.**    Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):   * **ICMP packets containing message “UDP port 53 unreachable length 254”.**   Note a likely cause of the incident:   * **No service was listening to the receiving DNS port. The next step is to identify whether the DNS Server is down or traffic to port 53 is blocked by the firewall.** |