# Cybersecurity Incident Report:

# Network Traffic Analysis

|  |
| --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log. |
| Network logs highlight a critical challenge: the inability to access port 53, the focal point for DNS service. Connecting attempts are met with silence, consistently triggering a "destination port unreachable" error.  **Key Points:**  **Port 53 Inaccessibility:**  Connecting to the DNS service on port 53 yields no response, resembling knocking on an unanswered door.  This triggers the consistent "destination port unreachable" error.  **Domain Address Blockage:**  Failing to reach port 53 impedes obtaining the address for "yummyrecipesforme.com," perpetuating the same error.  **Persistent Challenge:**  Despite multiple attempts, logs consistently flag the unavailability of port 53.  **Analysis Insights:**  Utilizing the UDP protocol for domain resolution reveals a breakdown when ICMP echo replies return the error message "destination port unreachable."  Port 53, crucial for DNS service, is highlighted in the error message, indicating its unavailability.  **Likely Cause:**  The primary issue stems from difficulties connecting to the DNS service on port 53. Potential causes include configuration confusion, inactive service, or rare interference.  **Recommended Actions:**  Urgent involvement of network experts is essential to investigate and rectify the port 53 connection issue.  Simultaneous engagement with security personnel ensures a thorough examination, addressing potential security implications.  Emphasis on proactive monitoring and maintenance of DNS infrastructure is critical for future prevention. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| **Time Incident Occurred:**  The incident unfolded at 13:24:32 marked by the initial UDP request seeking the IP address of "yummyrecipesforme.com."  **Awareness of the Incident:**  The IT team became aware when an access error surfaced, specifically the "destination port unreachable" message during attempts to access "yummyrecipesforme.com."  **IT Department's Investigative Actions:**  The IT department promptly responded by leveraging network analysis tools, including tcpdump, to capture and scrutinize data packets during subsequent attempts to load the webpage.  Special attention was given to discerning patterns in UDP packets and ICMP echo replies, particularly those returning the error message "udp port 53 unreachable."  **Key Findings of IT Investigation:**  The investigation underscored the persistent unreachability of port 53, a vital port for DNS service, in endeavors to communicate with the DNS server at IP address 203.0.113.2.  Salient details include recurring ICMP error responses indicating the DNS service's unavailability on port 53.  **Likely Cause of the Incident:**  A likely cause is associated with a potential misconfiguration or malfunction within the DNS server at IP address 203.0.113.2, specifically impacting its responsiveness on port 53. This could stem from service unavailability or improper configuration, impeding successful communication and DNS resolution.  **Next Steps:**  Our next steps involve checking the firewall to unblock port 53 for DNS communication. Simultaneously, we've contacted the web server's administrator to investigate signs of a potential attack collaboratively. We're scrutinizing firewall logs for security threats and ensuring transparent communication. Once resolved, we're implementing measures to prevent future incidents, including regular security checks and team training. The aim is not just fixing issues but ensuring our network's resilience. |