# Cybersecurity Incident Report:

# Network Traffic Analysis

| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log | |
| --- | --- |
| Summary of DNS and ICMP Traffic Log Analysis  The provided DNS and ICMP traffic log reveals a critical issue that is causing the inaccessibility of the website www.yummyrecipesforme.com. The analysis of the log indicates a problem with the DNS (Domain Name System) resolution process, which is preventing users from accessing the website. Here are the key points from the analysis:  DNS Requests: The log shows that multiple DNS requests were made from the source IP address 192.51.100.15 to the DNS server at 203.0.113.2. These requests were initiated to obtain the IP address of the domain name www.yummyrecipesforme.com.  ICMP Responses: In response to the DNS requests, the DNS server at 203.0.113.2 sent ICMP (Internet Control Message Protocol) responses. These ICMP responses contained an error message that indicated the unreachability of UDP port 53 on the DNS server.  UDP Port 53 Unreachable: The error message in the ICMP responses explicitly states "udp port 53 unreachable." This signifies that the DNS server's port 53, which is the standard port for DNS service, is not reachable. This is a crucial issue because port 53 is responsible for DNS communication, which is essential for translating domain names into IP addresses.  Repetitive Unreachability: The problem is consistent across multiple attempts. The same issue persists in subsequent DNS request attempts, with the DNS server consistently responding that UDP port 53 is unreachable.  Conclusion: The root cause of the problem lies in the inability to reach UDP port 53 on the DNS server. This unreachability is disrupting the DNS resolution process, which is necessary for users to access the website www.yummyrecipesforme.com. As a result, users are encountering the "destination port unreachable" error and are unable to load the website. The focus should be on addressing this port unreachability to restore normal website access for users.  In the subsequent steps, a deeper investigation will be required to identify the underlying causes of the unreachability of UDP port 53 and take appropriate actions to rectify the issue. | |
|

| Part 2: Explain your analysis of the data and provide one solution to implement |
| --- |
| Analysis of Data and Recommended Solution  Upon analyzing the provided DNS and ICMP traffic log, it's clear that the core issue revolves around the unreachability of UDP port 53 on the DNS server. This unreachability is preventing the successful DNS resolution process, leading to the "destination port unreachable" error when users attempt to access the website www.yummyrecipesforme.com. Here's a breakdown of the analysis and a proposed solution:  Analysis:  DNS Requests and ICMP Responses: The log indicates that DNS requests were initiated from the source IP address 192.51.100.15 to the DNS server at 203.0.113.2. In response, the DNS server consistently sent ICMP responses with the error message "udp port 53 unreachable."  Unreachability of UDP Port 53: The ICMP error message specifically mentions the unreachability of UDP port 53 on the DNS server. This is a critical issue because port 53 is essential for DNS service, which translates domain names into IP addresses.  Repeated Instances: The problem repeats across multiple attempts, indicating that the port unreachability is not an isolated incident. The DNS server consistently reports the same issue with every subsequent DNS request.  Proposed Solution:  Based on the analysis, one solution to implement is to investigate and address the underlying causes of the unreachability of UDP port 53 on the DNS server. Here's the recommended approach:  Solution: DNS Server Configuration and Firewall Review  Steps:  DNS Server Health Check: Perform a thorough health check of the DNS server at 203.0.113.2 to identify any underlying issues that might be causing the unreachability of UDP port 53.  Service Restart: If the DNS server is running as a service, attempt to restart the service. This might help in resolving any service-related issues that are causing the port unreachability.  Firewall and Network Configuration Review: Review the firewall rules and network configurations to ensure that port 53 is properly configured to allow incoming and outgoing traffic. Port 53 is a well-known port for DNS service and must be accessible for DNS resolution to work.  Collaboration with Network Team: Collaborate with the network team to identify any network-related issues that might be affecting the communication between the user's computer (192.51.100.15) and the DNS server (203.0.113.2).  Communication with Hosting Provider: If the DNS server is hosted externally, contact the hosting provider to address the issue from their end. They might need to adjust their network configurations to ensure proper DNS service functionality.  Testing and Monitoring: After implementing changes, conduct thorough testing to ensure that the DNS resolution process is functioning correctly. Monitor the network traffic to verify that the ICMP responses no longer report UDP port 53 unreachability.  Conclusion:  By addressing the underlying causes of the UDP port 53 unreachability on the DNS server and ensuring that the DNS service is properly configured and accessible, the issue should be resolved. This solution focuses on rectifying the core problem that is preventing DNS resolution and causing the "destination port unreachable" error for users attempting to access www.yummyrecipesforme.com. |