# Cybersecurity Incident Report:

# Network Traffic Analysis

|  |
| --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log |
| * Several customers contacted your company to report that they were not able to access the company website www.yummyrecipesforme.com, and saw the error “udp port unreachable” * The network protocol analyzer logs indicate that port 53 is unreachable after waiting for the page to load. Port 53 is normally used for HTTPS traffic. This may indicate a problem with the receiving DNS port as indicated by the ICMP error message which was not listening for some reason and therefore the message was not going not go through to the DNS server. * While it's difficult to pinpoint a specific attack based solely on this error message, one possible attack that could cause this error is a DNS-based Distributed Denial of Service (DDoS) attack. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide one solution to implement |
| * t's worth noting that this error message can also occur due to malicious or non-malicious reasons, such as network misconfigurations or connectivity issues between the client and DNS server. * If its malicious it is possibly an DNS-based Distributed Denial of Service (DDoS) attack. * The remaining lines in the log indicate that ICMP packets were sent two more times, but the same delivery error was received both times. error message: “udp port 53 unreachable.” * There are quite a few ways to tackle this issue such as increasing Network capacity, implement rate limiting mechanisms and traffic filtering, using DDoS mitigation services, using load balancing techniques and many others. |

## **Step 3: Provide a summary of the problem found in the DNS and ICMP traffic log**

Summary:

The DNS (Domain Name System) protocol is used for resolving domain names to IP addresses. In the log, we can see multiple DNS queries (A?) being sent from the source IP address 192.51.100.15 to the destination IP address 203.0.113.2, which is the DNS server. The DNS queries are for the domain name "yummyrecipesforme.com".

The ICMP (Internet Control Message Protocol) protocol is used for network troubleshooting and error reporting. In the log, we can see ICMP messages being sent from the destination IP address 203.0.113.2 to the source IP address 192.51.100.15. These ICMP messages indicate that the UDP port 53 (commonly used for DNS) on the destination IP address is unreachable.

Details:

* The source IP address 192.51.100.15 sends DNS queries for "yummyrecipesforme.com" to the destination IP address 203.0.113.2 repeatedly at different time intervals.
* The destination IP address 203.0.113.2 responds with ICMP messages indicating that the UDP port 53 (DNS) is unreachable.
* This pattern repeats multiple times in the log.

Interpretation:

The logs indicate that there are issues with resolving the domain name "yummyrecipesforme.com" using the DNS server at IP address 203.0.113.2. The ICMP messages suggest that the DNS server's UDP port 53 is unreachable, preventing successful DNS resolution. This can result in the inability to access the website or perform DNS-related operations for "yummyrecipesforme.com".

Based on the provided information, it is recommended to further investigate the DNS server configuration, network connectivity, and firewall settings to address the issue of the unreachable UDP port 53 and restore DNS functionality for the website.

Please note that this analysis is based on the provided log and additional information may be required for a comprehensive assessment.

## **Step 4: Explain your analysis of the data and provide one solution to implement**

Based on the previous analysis and the provided network traffic log, here is a description of the possible reasons behind the error messages and the incident scenario:

1. Problem first reported:

When the network traffic log captured DNS queries for the domain "yummyrecipesforme.com" and ICMP error messages indicating an unreachable UDP port 53.

2. Scenario, Events, and Symptoms:

The scenario involves a machine with a network traffic analyzer tool installed. Users of the machine reported difficulties accessing the website "yummyrecipesforme.com". The symptoms included unsuccessful DNS resolution for the domain and the inability to establish a connection to the website.

3, Information Discovered:

Upon investigating the issue, the network traffic log revealed repeated DNS queries for "yummyrecipesforme.com" sent from the source IP address 192.51.100.15 to the destination IP address 203.0.113.2 (DNS server). The log also showed ICMP error messages from the DNS server, indicating that the UDP port 53 (DNS) on the server was unreachable.

4. Current Status:

The current status of the issue is that the DNS resolution for "yummyrecipesforme.com" is **failing** due to the unreachable UDP port 53 on the DNS server.

5. Suspected Root Cause:

The ICMP error messages suggest that there might be a firewall or network connectivity issue preventing access to the DNS server's UDP port 53. It is possible that the server's **firewall** is blocking incoming traffic on port 53 or there could be **network configuration** issues causing the port to be unreachable.

6. Next Steps:

To troubleshoot and resolve the issue the following can be done:

* Verify the firewall settings on the DNS server to ensure that incoming traffic on port 53 is allowed.
* Check the network connectivity between the source machine (192.51.100.15) and the DNS server (203.0.113.2), ensuring that there are no network issues or misconfigurations.
* Investigate any recent changes or updates that might have affected the DNS server's accessibility.
* Monitor the network traffic and logs for further insights or patterns that could help identify the underlying cause.
* Collaborate with the network and system administrators to investigate and resolve the issue, considering additional diagnostic tools if necessary.

Please note that the above steps provide a general approach, and the actual troubleshooting and resolution process may vary depending on the specific network infrastructure and configuration in place.