Cybersecurity Incident Report

Subject: Incident Analysis Report - DNS Resolution Failure for www.yummyrecipesforme.com

Date: 23rd September, 2024.

Prepared By: Adjei Yaw Osei
Position: Cybersecurity Analyst

Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Summary of the Problem Found in the tcpdump Log

After analyzing the data presented in the tcpdump log, it is clear that the primary protocol producing the error message from the DNS server for the website www.yummyrecipesforme.com is **UDP**. This protocol is commonly associated with port 53, which is used for DNS queries.

Summary of tcpdump Log Analysis:

- The log shows multiple outgoing UDP requests to the DNS server (IP: 203.0.113.2) on port 53.

- Each of these requests is followed by ICMP error messages indicating "destination port unreachable."

Details Indicated in the Log:

- The source IP address is consistently 192.51.100.15, and the destination IP is 203.0.113.2.

- The logs capture repeated instances of ICMP errors that indicate the DNS server is not responding on the expected port.

Interpretation of Issues Found in the Log:

- The persistent ICMP errors suggest that the DNS server is either down or misconfigured, preventing successful communication for DNS resolution requests.

Part 2: Analysis of the Data and Proposed Solution

When the problem was first reported:

- The problem was first reported at 1:24 p.m.

Scenario, Events, and Symptoms Identified:

- Multiple clients reported being unable to access the website www.yummyrecipesforme.com, leading to an investigation by the IT team.

Current Status of the Issue:

- The IT team has identified that DNS queries are failing due to ICMP error messages indicating that the server is unreachable on port 53.

Information Discovered While Investigating:

- The tcpdump analysis revealed repeated ICMP errors related to port 53, confirming that requests to the DNS server are not being fulfilled.

Next Steps in Troubleshooting and Resolving the Issue:

1. Check the operational status of the DNS server at 203.0.113.2.

2. Review firewall configurations to ensure that UDP traffic on port 53 is allowed.

3. Investigate for any network outages or misconfigurations that could be impacting the DNS service.

Suspected Root Cause of the Problem:

- The DNS server may be down, misconfigured, or possibly blocked by a firewall, preventing it from responding to DNS queries. Further investigation is necessary to confirm this root cause.