Cybersecurity Incident Report: Network Traffic Analysis

Date: 3 May 2025
Author: Kashish Patiyal
Incident Type: Network Service Disruption
Target: www.yummyrecipesforme.com
Tool Used: tcpdump

Overview

A group of customers reported an inability to access the website www.yummyrecipesforme.com, receiving a **"destination port unreachable"** error. As a cybersecurity analyst, I investigated the issue by capturing and analyzing network traffic using tcpdump. The objective was to identify the affected protocol and determine the root cause of the service disruption.

Packet Capture Summary

During traffic simulation and capture:

- A **DNS query** was sent from the client (IP: 192.51.100.15) to the DNS server (IP: 203.0.113.2) using **UDP port 53**.
- Instead of a valid DNS response, the server returned repeated **ICMP "Port Unreachable"** errors:

  ICMP 203.0.113.2 > 192.51.100.15: udp port 53 unreachable

- The error indicated that **UDP packets targeting port 53 were not accepted**, meaning the DNS service was unreachable.

Technical Analysis

- The ICMP message is triggered when the destination port is not accepting traffic—indicating that no service was listening on UDP port 53.
- The communication protocol involved was UDP, used by DNS services.
- Multiple identical ICMP errors were recorded, confirming persistent failure in DNS resolution.

Root Cause Hypothesis

Based on the analysis, the root cause appears to be the **unavailability of DNS services** at the destination server. This could be due to:

- DNS service being **down or misconfigured**,
- A **firewall rule** blocking inbound traffic to port 53,
- A potential **denial-of-service (DoS) attack** targeting the DNS server,
- Or a **temporary network disruption** between the host and the DNS server.

Impact

- Users could not resolve the website domain to an IP address.
- Website remained inaccessible due to failed DNS resolution.
- Highlighted the importance of DNS availability for service uptime.

Recommendations

- Ensure DNS service is running and properly configured.
- Verify firewall rules to allow UDP traffic on port 53.
- Monitor DNS server availability using tools like Nagios or Zabbix.
- Enable logging and alerts for ICMP errors to flag potential DNS issues.
- Investigate and mitigate potential DoS attempts on DNS infrastructure.

Conclusion

The **DNS service using UDP protocol on port 53** was affected during this incident. The ICMP error message was instrumental in identifying the unreachability of the DNS server. This analysis demonstrates the importance of network traffic monitoring and the role of ICMP in diagnosing service-level disruptions.