

Cybersecurity Incident Report:

Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.

The tcpdump log shows repeated DNS resolution failures when attempting to access www.yummyrecipesforme.com. DNS queries were sent from the client to the DNS server using the **UDP protocol on port 53**. Each request resulted in an **ICMP error message** stating “**udp port 53 unreachable**.”

The protocols involved in this incident include **DNS** (domain name resolution), **UDP** (transport protocol used by DNS), and **ICMP** (used to report network delivery errors). The repeated ICMP responses indicate that the DNS service was unavailable, preventing the website’s domain name from being resolved and making the website inaccessible.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.

Time incident occurred:

The issue was first observed at approximately **13:24 (1:24 PM)**, based on the earliest timestamp in the tcpdump log.

How the incident was identified:

Customers reported receiving a “destination port unreachable” error when accessing the website. The issue was confirmed by the analyst and investigated using **tcpdump**.

Investigation findings:

- DNS queries were sent using **UDP to port 53**.

- The DNS server responded with **ICMP “udp port 53 unreachable”** messages.
- The error occurred repeatedly, indicating a persistent service issue.

Likely root cause:

The **DNS service was a victim of a DOS attack, misconfigured, or blocked by a firewall**, resulting in no service listening on UDP port 53.

Next steps:

- Verify that the DNS service is running on the server.
- Check firewall rules to ensure UDP port 53 is allowed.
- Monitor traffic to confirm successful DNS resolution after remediation.