# Cybersecurity Incident Report:

# Network Traffic Analysis

| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log. | |
| --- | --- |
| The UDP protocol reveals that:  The client **192.51.100.15** sent DNS **A**-record queries to **203.0.113.2** over **UDP port 53** for *yummyrecipesforme.com*, and each attempt was followed by an ICMP message indicating the port was unreachable.  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message:  udp port 53 unreachable  The port noted in the error message is used for:  **DNS** name resolution (**UDP/53**, with TCP/53 as fallback).  The most likely issue is:  the DNS resolver at **203.0.113.2** is **not reachable on UDP/53** (service down or **firewall/ACL blocking** the traffic), causing name resolution to fail and preventing access to the website. | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| Time incident occurred:  Multiple attempts between **13:24:32** and **13:28:50**; first ICMP failure observed at **13:24:36**.  Explain how the IT team became aware of the incident:  **Customers reported** they couldn’t reach *www.yummyrecipesforme.com*. Internal testing reproduced the issue.  Explain the actions taken by the IT department to investigate the incident:   1. Attempted to load the site while running a **tcpdump** capture. 2. Reviewed packets for **DNS queries** and subsequent **ICMP** responses. 3. Correlated the errors with the destination **DNS resolver (203.0.113.2)** and **port 53/UDP**. 4. Verified that web (HTTPS) traffic never started because **name resolution failed first**.   Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):   * Source host: **192.51.100.15** → Destination DNS: **203.0.113.2** * Protocol/port: **UDP/53 (DNS)** * Query: **A? yummyrecipesforme.com** * Response: **ICMP “udp port 53 unreachable”** from **203.0.113.2** to **192.51.100.15** * Pattern: error repeated across multiple attempts → systemic issue.   Note a likely cause of the incident:  **DNS service unreachable on UDP/53**—either the resolver on **203.0.113.2** is **down/not listening**, or **firewall/ACL rules** are **blocking UDP/53** between the client and the DNS server. |