## **Cybersecurity Incident Report by given Scenario (Google Certificate)**

### **Summary of the problem found in the DNS and ICMP traffic log**

The UDP protocol reveals that DNS requests sent from the client (IP 192.51.100.15) to the DNS server (IP 203.0.113.2) using UDP port 53 consistently failed. In response, the DNS server returned ICMP error messages: “udp port 53 unreachable.”

This is based on the results of the network analysis, which show that the ICMP responses were sent by the DNS server to the client IP. These messages contain the error “port 53 unreachable,” which indicates that the DNS server is not responding to queries using the DNS protocol over UDP.

The port noted in the error message is **UDP port 53**, which is used for **DNS (Domain Name System)** resolution.

The most likely issue is that the DNS server at 203.0.113.2 is either **not functioning**, **not reachable over UDP**, or **blocking port 53**. As a result, clients attempting to resolve the domain name **yummyrecipesforme.com** are receiving ICMP responses indicating that the DNS request could not be processed, which causes the browser to show “destination port unreachable.”

### 

### **Analysis of the data and cause of the incident**

**Time incident occurred:**

The issue occurred at several timestamps including 13:24:32, 13:26:32, and 13:28:32 (as shown in the tcpdump logs). Each attempt was met with the same ICMP error.

**How the IT team became aware of the incident:**

Multiple clients reported that they were unable to access the company website **yummyrecipesforme.com**. They reported receiving a “destination port unreachable” error after the website failed to load.

**Actions taken by the IT department to investigate the incident:**

The IT team captured network traffic using the tcpdump tool and analyzed outgoing DNS requests from the client to the DNS server. They examined the DNS request packets and the corresponding ICMP error responses using network layer inspection.

**Key findings:**

* DNS queries were initiated by the client to the DNS server using UDP port 53.
* The DNS server responded with ICMP packets indicating "udp port 53 unreachable."
* This pattern repeated for multiple attempts to access the domain **yummyrecipesforme.com**.
* No successful DNS resolution occurred, meaning the client never received the IP address of the target domain.

**Suspected root cause of the issue:**

The DNS server at **203.0.113.2** is either **down**, **blocking incoming UDP traffic on port 53**, or **misconfigured** (no DNS service is listening on that port). This prevents successful name resolution for the client.

## **Proposed Solution:**

**Immediate step:** Update the client system or firewall settings to use a different, functioning DNS server — such as **Google DNS (8.8.8.8)** or **Cloudflare DNS (1.1.1.1)** — to bypass the unreachable server.

**Longer-term fix:**

* Investigate the DNS server (203.0.113.2) to ensure the DNS service is running and accessible over UDP port 53.
* Review firewall rules and access control lists to ensure port 53 is not being blocked.
* Monitor DNS server logs for any recent errors or misconfigurations.
* Add DNS service health checks to the monitoring system to detect similar failures in the future.