Cybersecurity Incident Report: Network Traffic Analysis

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

Incident Summary:

The user experienced an inability to access the domain yummyrecipesforme.com. A packet capture analysis using tcpdump revealed repeated **ICMP error messages** indicating that **UDP port 53 was unreachable** on the DNS server (203.0.113.2). This prevented DNS resolution, blocking access to the requested website.

Impacted Network Protocol -> UDP (User Datagram Protocol)

UDP is a lightweight, connectionless transport layer protocol used for fast data transmission, commonly used with services where speed matters more than reliability.

Impacted Service -> DNS (Domain Name System)

Port **53** is specifically reserved for **DNS** traffic — the service that translates domain names (like google.com) into IP addresses.

Technical Findings:

- **Source IP:** 192.51.100.15 (client)
- **Destination IP:** 203.0.113.2 (DNS server)
- **Protocol used:** UDP
- **Port affected:** Port **53** (standard for DNS queries)
- **Error received:** ICMP: udp port 53 unreachable
- **Service impacted: DNS** (Domain Name System)
- **Domain being queried:** yummyrecipesforme.com

The UDP protocol reveals that:

The client at IP address 192.51.100.15 tried to send a DNS query over UDP to the DNS server at IP 203.0.113.2 using port **53**, which is the standard port for DNS services.

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", which indicates that the DNS server could not process the request. This is because it is either:

A] **Down**

B] **Not configured to accept on port 53**, or because

C] The **firewall settings** are blocking access.

The port noted in the error message is used for:

DNS (Domain Name System) queries, which are essential for resolving domain names (like yummyrecipesforme.com) into IP addresses.

The most likely issue is:

The DNS server at 203.0.113.2 is either **not running a DNS service**, the **service is misconfigured**, or **network/firewall settings** are blocking access to UDP port 53, preventing proper name resolution.

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

Time incident occurred:

- First error at: 13:24:36
- Repeated attempts: 13:27:15 and 13:28:50

Explain how the IT team became aware of the incident:

A user reported being unable to access the website yummyrecipesforme.com. The IT team then ran a tcpdump packet capture for DNS-related traffic and reviewed ICMP messages.

Explain the actions taken by the IT department to investigate the incident:

1.Captured and analyzed DNS queries and ICMP responses

2.Identified repeated attempts to reach the DNS server at 203.0.113.2

3.Observed that all attempts returned **ICMP "port unreachable"** errors for **UDP port 53**

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):

1.DNS queries sent from client 192.51.100.15 to DNS server 203.0.113.2

2.DNS server responded with **ICMP Type 3, Code 3** messages indicating **UDP port 53 unreachable.**

ICMP message type: 3 → Destination Unreachable

ICMP code: 3 → Port Unreachable

(From the ICMP message we can infer that it is type 3, code 3 from the “ICMP Type and code list”)

3. A record (A) was requested for yummyrecipesforme.com, but the DNS server was **unreachable or not listening on port 53**

Note a likely cause of the incident:

- The DNS service on 203.0.113.2 is **down or misconfigured**
- Blocked by a firewall or access control list (ACL)
  Network firewall rules may be blocking **UDP port 53**, either on the server itself or at an intermediate device (like a router or firewall).

Preventive Actions:

- Configure multiple DNS servers in client and network settings for **redundancy**
- Implement **monitoring and alerts** for DNS server health and port availability
- Periodically run **network health checks** using tools like: tcpdump, ping, etc
- Update firewall rules to prevent accidental blockage of essential services like DNS