Cybersecurity Incident Report

Network Traffic Analysis

Part 1: Summary of the Problem

The UDP protocol reveals that:

- The DNS request sent to resolve the domain "www.yummyrecipesforme.com" did not receive a valid response.
- The request was sent via UDP to the DNS server at IP address **203.0.113.2** on port **53**.
- The DNS query identification number was **35084**, and the request was for an A record resolution.

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:

- **Domain Name System (DNS) services**, which are responsible for translating domain names into IP addresses.

The most likely issue is:

- The DNS server at **203.0.113.2** is either down, misconfigured, or experiencing network issues, leading to a failure in domain resolution for "www.yummyrecipesforme.com."

Part 2: Analysis of the Data and Potential Cause of the Incident

Time incident occurred:

- **1:24 PM, 32.192571 seconds** (as indicated in the log timestamps).

How the IT team became aware of the incident:

- Multiple customers reported that they were unable to access the client website "www.yummyrecipesforme.com" and received a "destination port unreachable" error.
- Internal testing by the cybersecurity team confirmed the issue while attempting to access the website.

Actions taken by the IT department to investigate the incident:

1. Conducted network analysis using **tcpdump** to capture traffic between the local machine and the DNS server.
2. Verified that the UDP request to port 53 of **203.0.113.2** was sent but did not receive a valid DNS response.
3. Identified repeated **ICMP "udp port 53 unreachable"** messages in response to the DNS queries.
4. Confirmed that without DNS resolution, the HTTPS request to load the webpage could not be completed.

Key findings of the IT department's investigation:

- The affected protocol: **UDP (port 53 for DNS resolution)**.
- The affected DNS server: **203.0.113.2**.
- The affected service: **Domain Name System (DNS)**.
- The issue impacted **all users attempting to resolve the domain "www.yummyrecipesforme.com"**.

Likely cause of the incident:

- The DNS server **203.0.113.2** is unresponsive due to one of the following reasons:
    - **Server outage**: The DNS server may be offline due to maintenance, hardware failure, or software issues.
    - **Firewall misconfiguration**: A recent security policy update may have inadvertently blocked UDP traffic on port 53.
    - **DDoS attack**: The DNS server may be under a Denial-of-Service (DoS) attack, overwhelming it and preventing legitimate queries from being processed.
    - **Network misconfiguration**: A routing or ACL issue may be preventing access to the DNS server.

Next Steps:

- Escalate the issue to the **network and security engineering teams** for further investigation and remediation.
- Monitor DNS server availability and confirm if traffic filtering (firewall rules or IDS/IPS) is causing the issue.
- Provide an alternative DNS server for temporary resolution if necessary.
- Conduct a post-mortem analysis to identify root causes and implement preventive measures.

Conclusion:
The investigation confirms that the issue stems from the **inaccessibility of the DNS server at 203.0.113.2**, preventing domain name resolution for "www.yummyrecipesforme.com." Further analysis by the security engineers will determine whether this is due to **server failure, misconfiguration, or a potential cyber attack.**