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`) repeatedly sent DNS queries (UDP port 53) to resolve `yummyrecipesforme.com` but received no valid DNS responses. 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`, indicating the DNS server (`203.0.113.2`) could not process requests on UDP port 53. The port noted in the error message is used for: **DNS resolution** (UDP port 53), which translates domain names (e.g., `yummyrecipesforme.com`) to IP addresses. The most likely issue is: The DNS server's UDP port 53 was unavailable due to a **service outage** (e.g., DNS service not running) or **firewall misconfiguration** blocking access to the port.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: **13:24:32 to 13:28:50** (UTC), with three failed DNS queries logged over ~4 minutes. Explain how the IT team became aware of the incident: Users reported inability to access `www.yummyrecipesforme.com` and received `"destination port unreachable"` errors. The IT team reproduced the issue and confirmed it using `tcpdump` logs.

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

1. Captured network traffic with `tcpdump` during a webpage load attempt.
2. Analyzed logs and identified repeated DNS failures and ICMP errors.
3. Verified DNS server (`203.0.113.2`) status and checked firewall rules for UDP port 53.

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

- **Affected port**: UDP port 53 (DNS).
- **DNS server**: `203.0.113.2` was unresponsive to DNS queries.
- **Traffic pattern**: Three consecutive DNS requests triggered ICMP “port unreachable” errors.
- **No secondary DNS server**: Lack of redundancy worsened the outage.

Note a likely cause of the incident:

- **DNS service failure**: The DNS service on `203.0.113.2` was not running, or
- **Firewall misconfiguration**: A network security rule blocked UDP port 53, preventing DNS communication.

Summary of tcpdump Log Analysis

Protocols Identified:

- **DNS (UDP Port 53):** The client (`192.51.100.15`) repeatedly sent DNS queries to resolve `yummyrecipesforme.com` via UDP port 53.
- **ICMP:** The DNS server (`203.0.113.2`) responded with ICMP error messages indicating `udp port 53 unreachable`.

Key Details from the Log:

1. **Repeated DNS Queries:** Three consecutive DNS requests were made to the server (`203.0.113.2`) for `yummyrecipesforme.com` (e.g., `A? yummyrecipesforme.com.`).
2. **Consistent ICMP Errors:** Each DNS query triggered an ICMP response stating that UDP port 53 was unreachable.
3. **No Successful DNS Responses:** The log shows no valid DNS replies, only ICMP errors.

Interpretation of Issues:

- **DNS Server Failure:** The DNS server could not process requests on UDP port 53, likely due to:
    - The DNS service being offline or misconfigured.
    - A firewall/network rule blocking UDP port 53.

- **Impact:** Without DNS resolution, users could not access `www.yummyrecipesforme.com`, as the browser could not retrieve the website's IP address.

Conclusion:

The **DNS protocol (UDP port 53)** was directly affected, causing the "destination port unreachable" error. The ICMP error messages confirm the server's inability to handle DNS requests, leading to a complete failure in domain name resolution. This disruption explains the reported website inaccessibility.

Affected Protocol: DNS (UDP Port 53).
Root Cause: Unresponsive DNS server or blocked UDP port 53.

Cybersecurity Incident Report: Analysis and Resolution

1. **When the Problem Was First Reported**

    - **Time Reported:** The issue was first detected at **13:24:32 UTC** when users began experiencing website inaccessibility and received "destination port unreachable" errors.

2. **Scenario, Events, and Symptoms**

    - **Scenario:** Users attempted to access `www.yummyrecipesforme.com` but could not resolve the domain name.
    - **Events:**
        - The client (`192.51.100.15`) sent DNS queries (UDP port 53) to the DNS server (`203.0.113.2`) to resolve `yummyrecipesforme.com`.
        - The DNS server responded with ICMP error messages: `udp port 53 unreachable`, indicating it could not process requests on UDP port 53.
    - **Symptoms:**
        - Repeated DNS query failures over ~4 minutes (three attempts logged in the `tcpdump`).
        - No valid DNS responses, only ICMP errors.

3. Current Status of the Issue

- **Ongoing Outage:** The DNS server remains unresponsive on UDP port 53. Users still cannot access `www.yummyrecipesforme.com` due to unresolved domain resolution.

4. Information Discovered During Investigation

- **DNS Server Failure:**
  - The DNS server (`203.0.113.2`) is not accepting UDP port 53 requests.
  - Possible causes: DNS service is offline, misconfigured, or blocked by a firewall.
- **Lack of Redundancy:** No secondary DNS server was available to handle requests, exacerbating the outage.
- **Protocol Interactions:**
  - **DNS (UDP Port 53):** Used for domain resolution.
  - **ICMP:** Revealed the critical error `udp port 53 unreachable`, confirming the DNS server's inability to function.

5. Next Steps for Troubleshooting and Resolution

1. **Verify DNS Service Status:** Check if the DNS service is running on `203.0.113.2`. Restart it if necessary.
2. **Audit Firewall Rules:** Ensure UDP port 53 is not blocked by network security policies.
3. **Test Connectivity:** Use `nc -uvz 203.0.113.2 53` to confirm port availability.
4. **Implement Redundancy:** Deploy a secondary DNS server to prevent future outages.
5. **Monitor:** Set up alerts for DNS service health and port status.

6. Suspected Root Cause

- **Primary Cause:** The DNS service on `203.0.113.2` is either **not running** (e.g., crashed or stopped) or **blocked by a firewall rule.**
- **Contributing Factor:** Lack of a secondary DNS server created a single point of failure.

Conclusion

The ICMP error messages directly link the incident to UDP port 53 unavailability, halting DNS resolution for `yummyrecipesforme.com`. Restoring the DNS service or unblocking port 53 will resolve the immediate issue, while adding redundancy will mitigate future risks.

Solution to Implement

Restore DNS Service on UDP Port 53

- Restart the DNS service on `203.0.113.2` and verify port 53 is open in firewall rules.

Why This Works: Addressing the root cause (DNS service/port availability) ensures domain resolution resumes, allowing users to access the website. Proactive redundancy and monitoring prevent recurrence.