Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Summary of the Issue

Network analysis using `tcpdump` identified anomalies in DNS traffic. Specifically, multiple failed DNS lookup attempts were observed for `yummyrecipesforme.com` from `192.51.100.15:52444` to the DNS server `203.0.113.2:53`.

Each DNS request received an **ICMP "UDP port 53 unreachable"** error message, indicating that the DNS server was either unresponsive or misconfigured. This issue was recorded three times at **13:24:32.192571** with identical error responses.

Key Observations from Network Logs

- The affected protocol: **UDP (Port 53 - DNS)**
- Error message received: **"ICMP: UDP port 53 unreachable, length 254"**
- Frequency of occurrence: **Three consecutive DNS query failures**
- Possible causes:
    1. The DNS server at `203.0.113.2` is offline or not listening on port 53.
    2. Misconfiguration of DNS settings, such as missing or incorrect A records.
    3. A potential **Denial-of-Service (DoS) attack**, overwhelming the DNS server.

Screenshot of tcpdump log:

```
13:24:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:24:36.098564 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 254

13:26:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:27:15.934126 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 320

13:28:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:28:50.022967 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 150
```

Part 2: Incident Analysis

Time of Incident:

The incident was logged at **13:24:32.192571**, with three consecutive failed DNS queries.

How the Incident Was Identified:

Multiple users reported that they were unable to access the company's website, **www.yummyrecipesforme.com**. Attempts to reach the site resulted in a **"destination port unreachable"** error.

Investigation Steps by the IT Team:

1. **Initial Verification**: Attempted to access `www.yummyrecipesforme.com`, confirming the same error.
2. **Packet Capture & Analysis**: Used `tcpdump` to monitor network traffic and diagnose DNS failures.
3. **Key Findings:**
    - The DNS server at **203.0.113.2** failed to respond to lookup requests.
    - Instead of resolving the domain, an **ICMP error response** was returned, stating **"UDP port 53 unreachable."**
    - No valid **A record** was received for `yummyrecipesforme.com`.

Likely Root Cause of the Incident:

- The **DNS server is down** or misconfigured, leading to lookup failures.
- The **A record for `yummyrecipesforme.com` is missing or incorrect** in the DNS configuration.
- **Potential DoS attack**: If an attacker is overwhelming the DNS server with excessive requests, legitimate queries may fail.