Cybersecurity Incident Report

Part 1: Summary of the Problem (tcpdump log analysis)

After analyzing the captured tcpdump traffic, it was observed that DNS queries sent via UDP protocol from the client (192.51.100.15) to the DNS server (203.0.113.2) on port 53 were followed by ICMP error messages indicating the destination port was unreachable.

Protocols identified:

- UDP - Used for the initial DNS query to resolve the domain www.yummyrecipesforme.com.
- ICMP - Used for error messages returned to the client, indicating failure in UDP packet delivery.

Details from the log:

- At timestamp 13:24:32.192571, a UDP packet was sent to the DNS server on port 53.
- The response at 13:24:32.192726 was an ICMP message from the DNS server's IP, with the error: "udp port 53 unreachable."
- This pattern repeated in subsequent lines as the client retried the DNS query multiple times and received the same ICMP error.

Interpretation:

The DNS service on the server (203.0.113.2) is not responding on port 53, possibly because it is down, misconfigured, or not running. Because DNS resolution failed, the browser could not proceed to fetch the web page via HTTPS.

Part 2: Analysis and Proposed Solution

When the problem was first reported:

Cybersecurity Incident Report

The issue was first reported around 13:24 p.m. when users tried accessing the website and received a "destination port unreachable" error.

Scenario, events, and symptoms:

- Several users were unable to access the website www.yummyrecipesforme.com.
- A "destination port unreachable" error appeared after page load attempts.
- Attempts to manually access the site reproduced the same error.
- Using tcpdump, we captured traffic to the DNS server and identified that DNS queries were not being answered.

Current status of the issue:

- DNS resolution fails due to port 53 being unreachable.
- ICMP responses confirm that the DNS server is not accepting UDP connections on port 53, which is critical for DNS service.
- Without a valid DNS response, the browser cannot resolve the IP address of the website and cannot load it.

Findings from investigation:

- DNS requests to 203.0.113.2 are consistently rejected.
- ICMP messages confirm UDP port 53 is not listening or blocked.
- This indicates either the DNS server is offline, port 53 is blocked by a firewall, or the DNS service has failed.

Next steps to troubleshoot and resolve:

1. Check if the DNS server at 203.0.113.2 is operational.
2. Verify that DNS service (e.g., named, bind) is running on the server.

Cybersecurity Incident Report

3. Check firewall rules on the DNS server to confirm port 53 is not blocked.

4. Perform a port scan on 203.0.113.2 to confirm whether port 53 is open.

5. Restart the DNS service if it is found to be down.

6. Contact the server admin team if the server is managed externally.

Suspected root cause:

The DNS service on 203.0.113.2 is unreachable via UDP port 53, which is the standard port for DNS queries. This could be due to a service crash, port misconfiguration, or firewall blocking. As a result, users are unable to resolve the domain name, causing the website to be inaccessible.