**Cybersecurity Incident Report**

**Network Traffic Analysis**

**Part 1: Summary of the Problem Found in the tcpdump Log**

As part of the DNS protocol, the UDP protocol was used to contact the DNS server to retrieve the IP address for the domain name of yummyrecipesforme.com. The ICMP protocol responded with an error message, indicating issues contacting the DNS server. The UDP message from your browser to the DNS server is shown in the first two lines of every log event. The ICMP error response from the DNS server to your browser is displayed in the third and fourth lines of every log event with the error message, “udp port 53 unreachable.”

Since port 53 is associated with DNS protocol traffic, this indicates an issue with the DNS server. The flags associated with the UDP message, indicated by the plus sign after the query identification number 35084 and the “A?” symbol, confirm DNS protocol operations. Due to the ICMP error response message about port 53, it is highly likely that the DNS server is not responding. This is further supported by the flags associated with the outgoing UDP message and domain name retrieval.

**Part 2: Data Analysis and Possible Cause of the Incident**

**Time Incident Occurred:** The incident occurred today at 1:24 p.m. with the precise timestamp being 13:24:32.192571 for the initial request and subsequent timestamps for the ICMP error responses.

**How the IT Team Became Aware of the Incident:** Customers notified the organization that they received the message “destination port unreachable” when they attempted to visit the website yummyrecipesforme.com.

**Actions Taken by the IT Department to Investigate the Incident:**

1. The IT team attempted to visit the website and confirmed the "destination port unreachable" error.
2. They conducted packet sniffing tests using the network protocol analyzer tool, tcpdump, to capture and analyze the traffic between the client and the DNS server.
3. The team observed the outgoing UDP requests from the client to the DNS server and the ICMP error responses indicating issues with port 53.

**Key Findings of the IT Department's Investigation:**

* **Affected Port:** The error message "udp port 53 unreachable" indicated that the DNS server was not reachable on port 53.
* **DNS Server:** The server with IP address 203.0.113.2 was supposed to handle DNS queries but failed to do so.
* **Repeated Errors:** Multiple ICMP packets indicated that the issue persisted across several attempts to reach the DNS server.

**Likely Cause of the Incident:** The DNS server at IP address 203.0.113.2 was either down or misconfigured, leading it not to listen on port 53. The DNS service might have been disrupted due to a successful Denial of Service (DoS) attack or network misconfiguration. It is also possible that traffic to port 53 was blocked by a firewall.

**Conclusion**

The network protocol impacted during this incident was the DNS protocol over UDP. The error message "udp port 53 unreachable" indicates that the DNS server at 203.0.113.2 was not reachable on port 53, resulting in users being unable to resolve the domain name [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com) and encountering the "destination port unreachable" error.

**Recommendations**

* **Check DNS Server Configuration:** Ensure that the DNS server is correctly configured to listen on port 53.
* **Monitor DNS Server:** Implement monitoring tools to keep track of the DNS server's status and receive alerts if it goes down.
* **Investigate Network Issues:** Conduct a thorough investigation of the network to identify and resolve any underlying issues that might be affecting connectivity to the DNS server.
* **Evaluate Firewall Rules:** Check the firewall configuration to ensure it is not blocking traffic to port 53.

By addressing these recommendations, the availability and reliability of the DNS service can be improved, reducing the likelihood of similar incidents in the future.