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 shows that the DNS service was impacted during this incident. The network analysis shows that when a query was sent to the DNS server, an ICMP error message was returned stating, "udp port 53 unreachable." This indicates that the DNS server was not responding to requests, preventing users from resolving the domain name www.yummyrecipesforme.com to an IP address, and due to that, they were not able to access the website. 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.” This suggests that the DNS server at 203.0.113.2 was either down or misconfigured, leading to failed name resolution requests. The port noted in the error message is used for: DNS queries (port 53), which is the standard port for resolving domain names via the UDP protocol. The most likely issue is that the DNS server at 203.0.113.2 was either unavailable, misconfigured, or experiencing network connectivity issues, preventing users from resolving the domain name www.yummyrecipesforme.com. This resulted in failed HTTPS requests to load the webpage.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident occurred at 1:24 p.m., 32.192571 seconds, as indicated by the tcpdump log timestamps. The IT team was alerted to the issue when multiple customers reported being unable to access the website www.yummyrecipesforme.com. Users

encountered the error message “destination port unreachable,” prompting an investigation by the IT team.

The IT team tried to access the website to replicate the issue and confirmed the “destination port unreachable” error. They then used a network analyzer tool, tcpdump, to capture and analyze network traffic while trying to load the webpage. The analysis identified UDP requests to port 53 of the DNS server failing with ICMP responses indicating the port was unreachable. Multiple ICMP packets with the same error were observed, verifying the problem was not an isolated occurrence.

The affected port was UDP port 53, which is used for DNS resolution. The affected DNS server, 203.0.113.2, did not respond to queries. The ICMP error message indicated that no service was listening on UDP port 53, meaning the DNS server was either down or misconfigured. Without DNS resolution, clients were unable to retrieve the IP address of www.yummyrecipesforme.com, leading to website inaccessibility.

The most likely cause was a failure of the DNS service on the server on 203.0.113.2. Possible reasons include a DNS server outage, a misconfiguration where the DNS service stopped or the port was blocked, a firewall rule or network policy change preventing UDP traffic on port 53, or a DDoS attack or excessive traffic overwhelming the DNS service.

The IT department will escalate this issue to security engineers and network administrators to resolve the DNS server problem, restore normal operations, and implement measures to prevent future disruptions.