Cybersecurity Incident Report:
Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.

Upon reviewing the tcpdump log, we observed repeated attempts by the client IP address 192.51.100.15 to resolve the domain name yummyrecipesforme.com via DNS. These attempts used the UDP protocol, targeting port 53 on the DNS server at IP address 203.0.113.2. However, each DNS query was followed by an ICMP error response from the DNS server, indicating: "udp port 53 unreachable". This message means the DNS server was not listening or not reachable on UDP port 53, which is the standard port used for DNS queries. It is possible that this is an indication of a malicious attack on the DNS server.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.

The issue was first reported at 13:24:32, based on the timestamp in the tcpdump log.

Users attempted to access a website and were met with the error message “destination port unreachable.” When trying to load the page through a browser, there was no response or the connection failed. A tcpdump capture of the network traffic showed that DNS queries were being sent using the UDP protocol. However, the responses from the DNS server contained ICMP error messages indicating that UDP port 53 was unreachable.

The current status of the issue is that the DNS service required to resolve the website’s domain name is currently inaccessible or non-functional, which results in the website being unavailable to end users. The investigation into the root cause of the issue is ongoing, with efforts focused on determining how to restore access to the DNS server.

During the investigation, it was discovered that the DNS server at IP address 203.0.113.2 is not responding on UDP port 53. All DNS queries directed to this server are failing, and consistent ICMP error messages are being returned, indicating that the port is unreachable.

One Solution to Implement is to re-enable or restore UDP port 53 on the DNS server. This involves ensuring the DNS service is active, that the server listens on port 53, and that there are no firewall or routing rules blocking access. Alternatively, temporarily switch to a known reliable DNS server while the issue with the current DNS server is being resolved.