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 reveals that: The UDP message requesting an IP address for the domain ‘www.yummyrecipesforme.com’ did not go through to the DNS server because no service was listening on the receiving DNS port.

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.

The port noted in the error message is used for: Port 53 is a port for DNS service.

The most likely issue is: Server was down.

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

Time incident occurred: 13:24.

Explain how the IT team became aware of the incident: Several customers of clients reported that they were not able to access the client company website ‘www.yummyrecipesforme.com’, and saw the error ‘destination port unreachable’ after waiting for the page load.

Explain the actions taken by the IT department to investigate the incident: A cybersecurity analyst first confirmed the issue and then used the network analyzer tool ‘tcpdump’, to capture and analyze network traffic during another attempt to load the webpage.

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): The analysis of the captured packets showed that DNS queries sent via UDP from the Source IP ‘192.51.100.15’ to the DNS server at ‘203.0.113.2’ were failing. The server responded with an ICMP error message indicating that UDP port 53 was unreachable.

Note a likely cause of the incident: A likely cause of the incident could be because of a DDoS Attack to the Server.