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:
Communications intended for domain name resolution over port 53 are being sent out but are not being received by the DNS server.

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:
Domain Name System (DNS) service, which is responsible for translating human-friendly domain names to IP addresses.Domain Name System (DNS) service, which is responsible for translating human-friendly domain names to IP addresses.

The most likely issue is:
The DNS server at the IP address 203.0.113.2 isn't listening or responding on port 53, which is required for domain name resolution, or there might be a network configuration issue that is blocking UDP traffic on port 53.

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

Time incident occurred:
Starting from the timestamp 13:24:32.192571 as indicated in the logs.

Explain how the IT team became aware of the incident:
Several customers reported being unable to access the company website www.yummyrecipesforme.com and encountered the error "destination port unreachable."

Explain the actions taken by the IT department to investigate the incident:

- IT personnel attempted to visit the website and also encountered the error.
- Used the network analyzer tool, tcpdump, to inspect network traffic while attempting to load the webpage.
- Analyzed the captured data packets, particularly focusing on DNS requests and ICMP error responses.

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):

- Outgoing DNS requests were made from the source IP address 192.51.100.15 to the destination DNS server IP address 203.0.113.2 over UDP protocol and port 53.
- The ICMP responses from 203.0.113.2 indicated that port 53 was unreachable.
- The problem persisted even after multiple attempts, as ICMP packets were sent two more times with the same error.

Note a likely cause of the incident:

The DNS server associated with the IP 203.0.113.2 is either not configured to listen on port 53, or there are network issues or security policies in place blocking the traffic. This leads to an inability to resolve the domain name for www.yummyrecipesforme.com, resulting in the reported accessibility issue.