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 destination server is not responding to DNS queries on port 53, indicating that the service is unreachable.

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 DNS server is either down, misconfigured or blocked by a firewall.

The port noted in the error message is used for:
port 53 used for Domain Name System (DNS) queries which resolve domain names to IP addresses.

The most likely issue is:
The DNS server is either offline, not listening on port 53 or blocked by a firewall.

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

Time incident occurred:
The time the incident occurred was at 13:24:32 pm

Explain how the IT team became aware of the incident:
Several customers of client reported that they were unable to access client’s website, receiving a destination port unreachable error.

Explain the actions taken by the IT department to investigate the incident:
We have taken the following steps:

- Used tcpdump to analyse the network traffic.
- Sent a DNS query to verify if the website’s domain could be resolved.
- Checked ICMP responses and found that UDP port 53 is in fact unreachable.
- Verified DNS server status and checked firewall settings(This is inferred that the it department completed this step)

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

- The affected protocol is DNS(UDP port 53).
- The DNS Server at 203.0.113.2 was not responding queries.
- ICMP error indicated that UDP port 53 was unreachable.

Note a likely cause of the incident:

- The DNS server is down or misconfigured.
- A firewall rule may have blocked UDP traffic on port 53.
- The DNS service was not running on the server.

We are still currently investigating the root cause of the incident.