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: udp port 53 was unreachable when attempting to access the yummyrecipes website.

This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: the request was not delivered to the DNS port. This aligns with the fact that we see the ip address of the recipe website and then the .domain extension.
The port noted in the error message is used for: port 53 is a well known port for DNS service. Port 53 translates website names into IP addresses.

The most likely issue is: Problem with the DNS server. The DNS server is not listening to any requests. This may be due to the flooding of DNS requests to the server - rendering the service inoperable to websites that use it.

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

Time incident occurred: tcpdump recorded timestamp at 1:24:32 pm

Explain how the IT team became aware of the incident: Customers stated they could not reach the website. Also claimed that “destination port unreachable” as message after waiting for page to load.

Explain the actions taken by the IT department to investigate the incident: First, we scoped out the website and verified the complaints the customers were having. Then, we opened our packet analyzing tool to gather more information about the cause of this aberration.

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): UDP port 53 unreachable. DNS service provider is not listening to any requests to the receiving device. Website could not be loaded due to this.

Note a likely cause of the incident: May be due to firewall configuration. Firewall may be blocking requests to port 53. Or, the DNS server may be under DDoS attack.