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: port 53 is unreachable when trying to access the company website. 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: DNS communication. The most likely issue is: that the DNS server is down and not responding.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: in the afternoon. Explain how the IT team became aware of the incident: after several complaints from customers being unable to connect to the company website and reporting the same error message. Explain the actions taken by the IT department to investigate the incident: attempted to troubleshoot the problem by packet sniffing with network analyzer tool tcpdump. Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): tcpdump logs showed that when attempting to communicate with the DNS server on port 53, ICMP replied with an error message of “udp port 53 unreachable”. Note a likely cause of the incident: A likely cause of this incident may be in fact due to an overloaded server, which might be the result of some form of a DoS attack. Another likely cause may be simply a misconfigured firewall not allowing traffic to port 53.