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 port is unavailable** This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: **UDP port 53 is unreachable** The port noted in the error message is used for: **transmitting data that need to get to their destinations quickly, without the need for a connection** The most likely issue is: **the DNS server has been overwhelmed with requests**

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: **in the lunchtime hours at 13:24** Explain how the IT team became aware of the incident: **When customers complained that they could not reach their website, only receiving error messages, they informed the IT team** Explain the actions taken by the IT department to investigate the incident: **The department used network analyzing tool tcpdump to check which network port was affected during the attack, and as such found out that UDP port 53 was compromised** Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): **UDP port 53 was affected, taking down the DNS server and all its subsequent requests** Note a likely cause of the incident: **the DNS server might have been a victim of a 'Ping of Death' attack where an oversize ICMP packet was sent to the server. Another possibility is that the server was targeted by a denial of service attack which overwhelmed the network**