Cybersecurity Incident Report:
Network Traffic Analysis

Part 1: Summary of the problem found in the DNS and ICMP traffic log.
The UDP protocol reveals that: the DNS server is unreachable on port 53

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

The most likely issue is: DNS server not responding |

Part 2: Analysis of the data and cause of the incident.
The time incident occurred: 13:24 hours today.

The IT team became aware of the incident when several customers contacted the company to report that they were not able to access the company website www.yummyrecipesforme.com, and saw the error "destination port unreachable" after waiting for the page to load.

The actions taken by the IT department to investigate the incident include ongoing assessment and conducted a packet sniffing test using tcpdump

The IT department's investigation from the packet sniffing test found that DNS port 53 was unreachable.

Likely cause of the incident: DNS server might be down due to a successful Denial of Service attack. |