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 DNS server is down/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 port noted in the error message is used for DNS protocol traffic.

The most likely issue is that the DNS server is not responding.

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

The incident first occurred today at 13:24 in the afternoon.

The IT team became aware of the incident when customers contacted them to notify about an error “destination port unreachable” when attempting to access the website.

The network security professionals within the IT department first verified the error through the browser and once it was confirmed, conducted packet sniffing tests using tcpdump.

Following the packet sniffing tests, within the log file produced, we found that DNS port 53 was unreachable.

The next step is to identify whether the DNS server is down or if the traffic to port 53 is being blocked by the firewall.

The DNS server might be down due to a successful Denial of Service attack or a misconfiguration.