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 is 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 Domain Name System (DNS - resolves domains to IP addresses).

The most likely issue is that the message to request the IP address did not reach the DNS server, therefore the domain was unable to be resolved and the web browser was unable to obtain the IP address to access the site.

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

Time incident occurred: 13:24:32.192571

The IT team became aware of the incident after several customers of clients reported that they were not able to access the client company website “www.yummyrecipesforme.com” and saw the error “destination port unreachable” after waiting for the page to load.

The IT department began investigating the issue by first navigating to the site, on which they also received the error “destination port unreachable”. They then started packet capturing software (tcpdump) and attempted to access the site again while analysing the data packets.

On inspecting the captured packets, the IT team could see from the ICMP reply that the DNS server on port 53 was unreachable. The attempt to resolve the site address was made three times unsuccessfully.

Providing the firewalls are not blocking traffic to or from the DNS server, the lack of response could indicate that it has been misconfigured or is experiencing a successful denial of service attack.