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 website www.yummyrecipesforme.com can’t be reached and instead is showing a message that says “Destination port can’t be reached”.

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, to retrieve the relevant IP address for the entered URL of the website.

The most likely issue is that the said website or the web hosting service provider for the website is under a DoS attack.

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

Time incident occurred: 1:24 p.m.

Explain how the IT team became aware of the incident: Several customers contacted us saying they were not able to reach the said website and when one of our team members tried to reach the website he was also shown the same message as the other customers saying ‘destination port can’t be reached”.

Explain the actions taken by the IT department to investigate the incident: To investigate this incident the IT department used the network analyzer tool, tcpdump, to get the network logs.

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): During the investigation the IT department came to know that it was port 53, which is a well-known port for DNS, that was affected by this whole attack.

Note a likely cause of the incident: A likely cause of this incident could be a DoS attack.