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 request to gain access to the IP address for the domain was unsuccessful.

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: DNS service to provide the IP address for the website yummyrecipesforme.com.

The most likely issue is: an attack on the DNS server via flooding of network traffic which in turn leads to the server being unable to process requests as it will be overwhelmed.

Part 2: Analysis of the data and the likely cause of the incident.

Time incident occurred: 1:24pm, 32.192571 seconds

Explain how the IT team became aware of the incident: Clients of the company reported they were failing to access the website yummyrecipesforme.com.

Explain the actions taken by the IT department to investigate the incident: The IT department loaded up tcpdump to analyze the data packets on the network when they tried to access the website.

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): udp port 53 was the affected port, which is the port for the DNS server responsible for sending back the IP address for websites. The ICMP packet was undeliverable to the DNS server.

Note a likely cause of the incident: Network flooding is the likely cause of the incident.