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: It reveals that when user sends UDP packets to the DNS server, user receive ICMP packets containing the error message: “udp port 53 unreachable”.

This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: Port 53 is normally used for DNS name resolution, it converts name to IP address

The port noted in the error message is used for: The udp port 53 is used for DNS query, when a user search the website name in the search bar to translate name to IP address to access the website.

The most likely issue is: This might be possible attack has done on the DNS server to disrupt the services from accessing the server.

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

Time incident occurred: By looking at logs, findings say that timestamps that indicate the first sequence of numbers displayed : 13:24:32.192571, this means the time is 1:24 p.m., 32.192571 seconds.

Explain how the IT team became aware of the incident: Several customers of clients reported that they were not able to access the client company website www.yummyreclpesforme.com, and saw the error “destination port unreachable” after waiting for the page to load, through clients report analysts got aware of the incident.

Explain the actions taken by the IT department to investigate the incident: After knowing the reports from clients, analyst attempted to open the website to access but the result similar to clients. Then to troubleshoot the issue, analyst loaded network analyzer tool, tcpdump to capture the packets and find the cause if the incident. Then after trying to access the website, network analyzer captures the packets. With analysis of packets we can say that when we try to query the DNS it replied ICMP echo reply error message. So for many requests it ICMP echo reply is “udp port 53 unreachable”. The error message, “udp port 53 unreachable” in the message indicates the UDP message requesting an IP address for the domain did not go through to the DNS server because no service was listening on the receiving DNS port. So finally analysed that the DNS server was disrupted by attack.

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): The error message, “udp port 53 unreachable”, the port 53 is aport for DNS service. The “A?” indicates a flag associated with the DNS request for an A record, where an A record maps a domain name to an IP address.

Note a likely cause of the incident: The network security team suspects this might have launched an attack to crach the DNS server to stop the business operations.