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 DNS Server is down or unreachable, this is evident from the ICMP echo reply “

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 Resolution

The most likely issue is:

No service is listening on the receiving DNS port 53 on the 203.0.113.2.domain to fulfill the request from the host

Part 2: Explanation of analysis of the data and possible cause of the incident.

Time incident occurred: 1:24pm

Several customer reports stating they cannot access the website www.yummyrecipesforme.com and received the error destination port “unreachable”.

I Began my analysis into this by visiting the website myself to see if I can replicate the issue, I received the same error.

I then went on to use a network analysis tool (TCPDUMP) to capture the packets as they tried to connect to the web server, I had received an ICMP response noting port 53 was unreachable, this indicates that the host cannot connect to the DNS server, this could be due to an attack such as a Denial Of Service attack or a possible ICMP Flood attack that repeatedly sends ICMP packets to a network server.

Furthermore, a UDP packet was sent from the host device, an ICMP response returned to the host device, the result contains an error message “UDP port 53 unreachable”.

No service was running on the receiving port 53 which indicates a possible DOS/DDOS or ICMP flood attack on the web server to block legitimate requests to the websites.