Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.

The ICMP protocol reveals that: port 53 is unreachable when attempting to resolve the “yummyrecipesforme” domain name into its ip address.

The UDP message going from the browser to the DNS server is shown in the first two lines of every log event. The ICMP error response from the DNS server to the browser is displayed in the third and fourth lines of every log event with the error message, “udp port 53 unreachable.” Port 53 is commonly used for DNS resolution. The most likely issue is either a firewall configuration blocking traffic from port 53 or an attack on the DNS server such as DDoS attack that has taken the server offline.

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

The incident first occurred around 1:24 pm when I received the first error message while trying to access the website. I became aware of this issue after several customers of the client reported that they were unable to access the website and were receiving a port unreachable message. To investigate the issue, I tried to access the website while running tests with the network protocol analyzer tcpdump. Currently it seems that port 53 which is the port used for DNS resolution is unreachable. Our next steps are to check the firewall configurations to make sure that port 53 is not being blocked. If that is not the case then there would probably be an issue with the DNS server. It might have been the target of a DDoS attack. I will contact the server administrator to check.