Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
The network protocol analyzer logs indicate that port 53 (a DNS service port) is unreachable when attempting to query a DNS server via the UDP protocol to retrieve the IP address for the website's domain name www.yummyrecipesforme.com, this means that did not go through to the DNS server because no service was listening on the receiving DNS port. 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 it is the port most web applications expect to find DNS servers, which they use to translate domains into IP addresses. This may indicate a problem with the web server, this may be an indication of a malicious attack.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident occurred at 13:24:32.192571, which corresponds to 1:24 p.m. and 32.192571 seconds in the afternoon. The IT team was notified when multiple customers reported being unable to access the client's website, www.yummyrecipesforme.com. Users experienced a "destination port unreachable" error after waiting for the page to load. To confirm the issue, the IT team attempted to access the website directly and encountered the same "destination port unreachable" error. They initiated a network analysis using the tool `tcpdump` and attempted to reload the webpage, capturing data to diagnose the underlying problem. Analysis revealed that the browser first sends a DNS query to a DNS server using the UDP protocol to obtain the IP address of the website. Once the IP is received, the browser uses

it as the destination for an HTTPS request to load the page. However, `tcpdump` captured ICMP packets from the DNS server indicating "UDP port 53 unreachable," which suggests that DNS requests were unable to reach the intended port.

The investigation points to a potential Denial of Service (DoS) attack, where the network is overwhelmed by an excessive volume of data packets. This surge in unwanted traffic likely caused the DNS server to become unresponsive, preventing legitimate users from accessing the website.