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 port 53 is unreachable for users when they attempt to visit the yummyrecipesforme.com site. 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, Port 53, is primarily used to request the Domain Name System (DNS) to convert a domain name into the IP address for the website’s server. Given the circumstances, I believe there could be problems with the DNS server itself, firewall configurations, or potentially there are issues occurring during the TCP handshake process. It is possible that this is an indication of a malicious attack on the web server.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident occurred today at 1:24pm, customers proceeded to submit emails and calls to the organization, notifying the IT team about error messages they were receiving when attempting to open the site yummyrecipesforme.com. Per the customers’ report, they were being met with the error message “destination port unreachable” when trying to visit the site. After analyzing the network traffic using the tcpdump protocol analyzer, the cybersecurity analyst has confirmed that UDP port 53, used for DNS requests, is currently unreachable. Sending a UDP request to resolve the IP address for yummyrecipesforme.com returns an ICMP packet indicating that port 53 is not accessible. We are actively investigating the root cause of this issue to restore access to the site. Our next steps include reviewing the firewall configuration to ensure that port 53 hasn’t been inadvertently blocked and contacting the web server’s system administrator to check for any signs of an attack. All ICMP requests are also returning errors that indicate port 53 is unreachable, which could point to a potential Denial of Service (DoS) attack overwhelming the server with requests. The network security team will continue working to resolve the outage.