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: The DNS protocol uses the UDP protocol to communicate with the remote DNS server in order to obtain the IP address hosted on the domain yummyrecipesforme.com. The ICMP protocol was used to transmit an error message, informing that there are issues accessing the DNS server. 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 System (DNS) turns domain names into IP addresses. The most likely issue is: ICMP error response (udp port 53 unreachable) message about port 53, the likely issue is the DNS server is not responding.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: The incident occurred at 1:24 PM (13:24:32.192571 PM). Explain how the IT team became aware of the incident: Several clients reported that they were unable to access the company's website "www.yummyrecipesforme.com" and saw the error "destination port unreachable" after waiting for the page to load. Explain the actions taken by the IT department to investigate the incident: Sniffing tests were conducted using tcpdump to check for errors in the packet exchanges while loading the page. It was discovered that DNS port 53 was inaccessible. Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): In the resulting log file, are found that DNS port 53 was unreachable. The next step is to identify whether the DNS server is down or traffic to port 53 is blocked by the firewall. Note a likely cause of the incident: DNS server might be down (inativo) due to a successful Denial of Service or a misconguration.