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: UDP Port 53 is unreachable for users attempting to reach the company website www.yummyrecipesforme.com and were confronted with the error "destination port unreachable". 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: both TCP and UDP communication and is responsible for making outgoing connections for host name & IP address lookups. The most likely issue is: There may be a problem where the firewall is not allowing connections through this port, or possibly an IDS system could be identifying false-positives. It is also possible that this port is falling victim to a network attack, and should be investigated further to rule out this possibility.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: 1:24 p.m., 32.192571 seconds. Explain how the IT team became aware of the incident: The IT team became aware of the incident as many customers explained that they could not reach the company website. Explain the actions taken by the IT department to investigate the incident: The IT team first opened the website and was confronted with the same "destination port unavailable" error, which led them to open tcpdump to analyze traffic on the network. Upon reviewing the logs captured by the packet sniffer, the IT team discovered UDP port 53 to be unavailable. Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): The IT department was able to discover port 53 was unreachable.

Note a likely cause of the incident: Port 53 is unavaiable either through an overload in requests or because a firewall is blocking this port. The port being unavailable interrupts host name & IP address lookups, which causes the error for the customers attempting to access the site. It is imperative that firewall filters are reviewed as well as taking measures to investigate the possibility of a denial of service or other network attack.