Nicholas Coleman

Cybersecurity Incident Report: Network Traffic Analysis

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

As per the DNS protocol, the UDP protocol was used to contact the DNS server to retrieve the IP address for the client's website. The network protocol analyzer indicated that port 53 is unreachable when attempting to access the client's website. 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". Port 53 is used as the default port for DNS protocol traffic, so it being unreachable means there is most likely an issue with the DNS server.

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

The incident occurred at 1:24:32 P.M.The IT team became aware of the incident after several customers of the client were not able to access the client company website: "www.yummyrecipesforme.com". The webpage showed the error: "destination port unreachable". After being informed of the issue by the client, the IT team conducted a packet sniffing analysis using **tcpdump**. The resulting log files showed that DNS port 53 was unreachable.

Our next step is to ensure that network traffic going to port 53 is not accidentally being blocked by the firewall. If the issue still persists, then the DNS server itself is likely nonfunctioning at the moment. If the DNS server is down, in all likelihood the issue is a Denial of Service (DoS) attack that has overloaded the server with data and caused it to crash. If this is the case, the client will have to wait until the DNS server is up and running once again.