Cybersecurity Incident Report: Network Traffic Analysis

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

As part of the DNS protocol, the UDP protocol was used to contact the DNS server to retrieve the IP address for the domain name of the yummyrecipesforme.com . The ICMP protocol was used to respond with an error message, indicating issues contacting the DNS Server. The UDP message going from your browser to the DNS server is shown in the first two lines of every log event. The ICMP error response from the DNS server to your browser is displayed in the third and fourth lines of every log event with the error message, “udp port 53 unreachable.” The port 53 is used for translating the human-readable domain names (for example: yummyrecipesforme.com) into numerical IP addresses that the machines(computers) use to communicate. Therefore, this is an issue with the DNS Server. Issues with performing the DNS protocol are further evident because the plus sign after the query identification number 35084 indicates flags with the UDP message and the “A?” symbol indicates flags with performing DNS protocol operations. Due to the ICMP error response message about port 53, it is highly likely that the DNS server is not responding. This assumption is further supported by the flags associated with the outgoing UDP message and domain name retrieval.

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

Time incident occurred: Nearly at 1:24pm. Several clients reported that they were not able to access the client company website www.yummyrecipesforme.com, and saw the error “destination port unreachable” after waiting for the page to load. The cybersecurity team providing IT services to their client organization are currently investigating the issue so customers can access the website again. In our investigation into the issues, we conducted packet sniffing tests using tcpdump. The resulting logs reveal that the port 53 which is used by the DNS server to translate domain names into IP addresses, is unreachable. Our next step is to identify whether the DNS server is down or the traffic port 53 is blocked by the firewall. The DNS Server might go down due to a successful Denial of Service(DoS) attack or misconfiguration.