

Cybersecurity Incident Report:

Network Traffic Analysis

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

The network protocol analyzer logs indicate ICMP error message “udp port 53 is unreachable” when attempting to request an ip address of domain name “yummyrecipesforme.com”. Port 53 is generally used for DNS protocol traffic. we know 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.

The incident occurred today at 1:24 p.m. when Several customers of clients reported that they received the message “destination port unreachable” while trying to access website www.yummyrecipesforme.com. The network security team responded and began running tests with the network protocol analyzer tool tcpdump. The resulting logs revealed that port 53, which is used for DNS server, is not reachable. We are continuing to investigate the root cause of the issue to determine how we can restore access to the website. The next step is to identify whether the DNS server is down or traffic to port 53 is blocked by the firewall. The DNS server might be down due to a successful Denial of Service attack or a misconfiguration.