

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 indicate that port 53 is unreachable when attempting to request access to website - yummyrecipesforme.com
Port 53 is commonly used for TCP and UDP communications. This may indicate a problem with the DNS not listening/receiving communications to port 53.

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

The incident occurred later in the day when several customers of clients reported that they were unable to access the client company website. The IT team responded and began tests with network protocol analyzer tool tcpdump. The resulting logs revealed that port 53, which is used for TCP and UDP communications, is not reachable. We are continuing to investigate the root cause of the issue to determine how we can restore access to the website for customers. Our next steps include checking to see if port 53 is blocked and check systems for signs of DOS attack.