

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 that port 53 is unreachable when attempting to access the company website www.yummyrecipesforme.com. Port 53 is normally used for DNS service. This may indicate a problem with the DNS server. It is possible that the DNS server is not responding.

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

The incident occurred earlier this afternoon before 1:24pm, when several customers contacted our company to report that they were not able to access our company website and kept receiving the message "destination port unreachable". The network security team responded by visiting the website, then began running tests with the network protocol analyzer tool tcpdump. The resulting logs revealed that port 53, which is used for DNS service, is unreachable. We are continuing to investigate the root cause of the issue so that customers can access the website again. Our next steps include checking the firewall configuration to see if port 53 is blocked and identify whether the DNS server is down. The DNS server might be down due to a misconfiguration or a successful Denial of Service attack.