

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 ip address of the website in DNS. Port 53 is normally used for UDP or TCP connections to the server. This may indicate a problem with the Domain name server or UDP. It is possible that this is an indication of a malicious attack on the website.

Part 2: Explain your analysis of the data and provide one solution to implement

The incident occurred when the customers reported that they could not reach the company website and saw the error "destination port unreachable". 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 UDP/TCP connections, is not reachable. We are continuing to investigate the root cause of the issue to determine how we can restore access to the secure website. Our next steps include checking the firewall configuration to see if port 53 is blocked and contacting the system administrator for the web server to have them check the system for signs of an attack.