

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 443 is unreachable when attempting to access the secure employee background check website. Port 443 is normally used for HTTPS traffic. This may indicate a problem with the web server or the firewall configuration. It is possible that this is an indication of a malicious attack on the web server.

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

The incident occurred today at 1:23 p.m.. Customers called the organization to notify the IT team that they received the message “destination port unreachable” when they attempted to visit the website. The network security professionals within the organization are currently investigating the issue so customers can access the website again. In our investigation into the issue, we conducted packet sniffing tests using tcpdump. In the resulting log file, we found that DNS port 53 was unreachable. 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.