# Cybersecurity Incident Report:

# Network Traffic Analysis

Scenario:

This issue was a situation with a port issue with a company website that needed help investigating potential malicious network activity traffic to detect a potential threat within the protocol. This incident report breaks down the methods used to find the potential threat activity that was detected within this process.

|  |
| --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log. |
| The UDP protocol reveals that:  The network protocol analyzer logs showed that port ‘53’ is unreachable when attempting to access a secure connection for the company website. Port ‘53’ is primarily used for DNS which is a standard port destination. DNS client applications use DNS protocol to query and request information from DNS servers and the servers return results back to the client using the same port. Port 53 is also used for both TCP/UDP communication. What this error message revealed was the port ‘53’ was not able to reach a secure connection to be built for the website to display on the webpage screen.  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message:  The error message was displayed as “udp port 53 unreachable”  The port noted in the error message is used for:  **DNS standard port destination usage and TCP/UDP communication protocol for network traffic.**  The most likely issue is:  **UDP port 53 is malfunctioning where the DNS/IP address are not communicating effectively to establish a secure connection for the company client website to produce the site’s functionality to exist on the webpage screen.** |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred:  The incident occurred at 1:24PM  **Explain how the IT team became aware of the incident:The IT team was aware of the situation when consumer clients were reporting complaints on the company website. The consumers complained that there was an error message displayed on the website saying “destination port unreachable”. The customers were not able to gain access to the website at all at the time of the issue.**  **Explain the actions taken by the IT department to investigate the incident:**  **The IT department tasked me to run an analysis on the issue using a network analyzer tool and tcpdump to reload the website again. Once that occurred we noticed a bunch of data packets shown from the network analyzer. The analyzer showed lots of data packets when it displayed UDP packets, and an ICMP message response came back to the network host. This issue led to the error message “udp port 53 unreachable” to occur during this manner.**  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):  Note a likely cause of the incident:  **The main cause of this issue could have been a firewall or filtering router that is blocking connections to port 53 on the host for both UDP and TCP connections. The firewall configuration must permit connections on this port from any host on the Internet for the DNS to function properly. If this is to be removed this could be the solution to fix the problem. Certain UDP ports could be blocked by firewall security properties configured on the computer that result in such a manner for this to happen.** |