# Cybersecurity Incident Report:

# Network Traffic Analysis

|  |
| --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log. |
| The UDP protocol reveals that: Port 53 is unresponsive on the destination side  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: “UDP Port 53 unreachable length 254”  The port noted in the error message is used for: Domain Name System (DNS) Service  The most likely issue is: The Port on the destination Host is not open or is not responding, either the system is down or the port is not set to receive traffic. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred: Incident occurred at 01:27 PM and 36.098564 Seconds.  Explain how the IT team became aware of the incident: IT Team became aware of this incident due to customer reporting that the company website was inaccessible.  Explain the actions taken by the IT department to investigate the incident: Actions taken was to visit the website which returned the error “destination port unreachable.” Next was to load the Network Analyzer tool with the command tcpdump and loading the webpage again which shows the error messages.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): Key is that the Port 53 is unreachable and needs to either be opened or investigated for rules on why it is not allowing traffic.  Note a likely cause of the incident: Port 53 is not allowing traffic and rules need to be investigated on if a new ruleset needs to be enabled on the host server or not. |