# 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: the DNS service that the web site is attempting to reach is unavailable to service the HTTPS request to access the website during rsolution from ip to hostname in order to resolve the website.  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 xxx**  The port noted in the error message is used for: **DNS in order to translate ip address of the website to its domain name.**  The most likely issue is: **a network issue with the client company website** |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred: **13:24**  Explain how the IT team became aware of the incident: We were made aware of this issue when users escalated this issue to our department stating that they were unable to access the website stating that it was not loading.  Explain the actions taken by the IT department to investigate the incident: tcp dump packet analyzer was used to establish what is ocuring. We also tested the website navigation on the browser wher we rceived the same error message as reported from the impacted users.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): Acording to the findings requestor ip is unable to receive data packets on port 53 in order to access the website  Note a likely cause of the incident: there could be a misconfiguration on the client's firewall preventing traffic requests on port 53 or there could potentially be an attempt of a DOS attack from malicious individuals attempting to bring DNS service to a halt |