# 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: Upon requesting information for the website port 53 has been shown to be unreachable. Port 53 is responsible for DNS & the ICMP reply has returned UDP port 53 is unreachable, high possibility of DNS server not responding.  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: Port 53 unreachable  The port noted in the error message is used for: DNS  The most likely issue is: DNS server being down | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| Time incident occurred: Timestamp shows incident occurred at 1:23 PM  Explain how the IT team became aware of the incident: Multiple customers had contacted the organization stating their website hadn’t been loading and returning the error message ‘destination port unreachable’  Explain the actions taken by the IT department to investigate the incident: The IT department decided as a first step was to use tcpdump and see if there was any suspicious activity. Upon the results of the dump within the log file they had discovered that port 53 was unreachable. With this information they checked if the entire DNS was down or if it was just blocked by a firewall, the DNS could be down due to a denial of service attack or a simple misconfiguration.  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: |