# Cybersecurity Incident Report:

# log from tcpdump packet dataNetwork Traffic Analysis

|  |
| --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log. |
| The analyzer logs indicate that UDP protocol was used for the request with port 53. ICMP return of the error message indicates that UDP port 53 was unreachable, meaning that the DNS server was not listening through the port. This may have happened because of a DoS attack that kept the DNS server busy. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| The incident first occurred around 13:24 when a customer could not access the company website and they saw the error “destination port unreachable” after waiting for the page to load. IT team used tcpdump network protocol analyzer tool to check logs. The logs revealed that the UDP protocol with port 53 could not reach the DNS server. Reason for this was because the DNS server was not listening the port. Investigation of the issue and ways to restore access to the company page continues. In the next step, port 53 will be checked to see if the port was blocked and the system will be checked to see if any signs of an attack exists. It is possible that a random hacker or a hacker hired by a rival company may have performed this attack to damage the company and its reputation. |