# 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 indicates that port 53 is unreachable when attempting to access the secure company website. Port 53 is commonly used for DNS TCP protocol. This might indicate that the issue is about not being able to establish a connection with the server, meaning the DNS server is down. | |
|

| Part 2: Explain your analysis of the data and provide one solution to implement |
| --- |
| The incident happened today at 1:23 p.m. and customers called the organization to notify the IT team that they received the message “destination port unreachable” after attempting to enter the website. In our investigation into the issue. Our next steps include conducting packet sniffing tests using tcpdump. In the resulting log file, we found that DNS port 53 was unreachable. The DNS server might be down due to a successful Denial of Service (DoS) attack, a SYN Flood attack, or an internal error unrelated to an attack. The next step is to identify whether the DNS server is down or if traffic to port 53 is blocked by the firewall. The network security professionals are currently investigating the issue to fix the website access for the customers. |