# Cybersecurity Incident Report:

# Network Traffic Analysis

| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log. | |
| --- | --- |
| The network protocol analyzer revealed that UDP port 53 is unreachable when attempting to access the company website. Based on the ICMP “UDP port 53 unreachable ” error message received. UDP port 53 is used for DNS. This may indicate a problem with the web server or the firewall configuration. | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| The incident occurred at 1:24 p.m, the security team was notified by a customer calling in to report an error message “destination port unreachable” displaying when loading the company website. The security team visited the website and received the same error “destination port unreachable”. The team then ran a network protocol analysis using TCPdump. The ICMP log result identified that UDP port 53, which is used for DNS, is unreachable. The next step is to identify whether the DNS server is down or traffic to port 53 is blocked by the firewall. The likely cause is a successful DoS attack on the DNS server. |