# 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 shows that the DNS server is either down or inaccessible. Network analysis results back this up with the ICMP echo reply error, “UDP port 53 unreachable.” Since port 53 is primarily for DNS traffic, it's very likely the DNS server isn't responding. | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| Today at 1:23 p.m., customers alerted the organization that they received a "destination port unreachable" message when trying to visit the website. Network security professionals are now investigating so customers can regain access. During our investigation, we conducted packet sniffing tests using tcpdump and found that DNS port 53 was unreachable. The next step is determining whether the DNS server is down or if the firewall is blocking traffic to port 53. The DNS server may be down due to a successful Denial of Service attack or a misconfiguration. |