# 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 logs indicate that port 53 is unreachable when several customers attempt to access the company’s website. Port 53 is normally used for  TCP and UDP communication. This may indicate that the packet size is too large to push through in a single UDP packet.  It is possible that this is an indication of a malicious attack on the web server. | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| The incident occurred earlier this morning when the customer reported that they were not able to reach the web portal. The network security team  responded and began running tests with the network protocol analyzer tool tcpdump. The  resulting logs revealed that port 53, which is used for UDP andTCP connection, is not established. We  are continuing to investigate the root cause of the issue to determine how we can restore  access to the secure web portal. Our next steps include checking the firewall configuration to see if port 53 is blocked and contacting the system administrator for the web server to have them check the system for signs of an attack. The  network security team suspects that DDOS attack may have taken place to crash the  website. |