# Cybersecurity Incident Report

| Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log |
| --- |
| The tcpdump packet capture logs indicate that port 53 is unreachable when attempting to access through ICMP protocol. Port 53 is normally used for DNS traffic. This may indicate a problem with the DNS server. It is possible that this is an indication of a malicious attack on the DNS server. |

| Part 2: Explain your analysis of the data and provide at least one cause of the incident |
| --- |
| The incident occurred this afternoon when we received several reports of customers unable to access the company website. 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 DNS traffic, is not reachable. We are continuing to investigate the root cause of the issue to determine how we can restore access to the DNS server. Our next steps include checking the firewall configuration to see if port 53 is blocked and contacting the system administrator for the DNS server to have them check the system for signs of an attack. The network security team believes that this may be an indication of DoS attack on the DNS server. |