# 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 reveals that the DNS server is either down or unreachable. Attempting to reach our website returns the error “UDP port 53 unreachable”. Port 53 is in charge of our DNS protocol traffic. This most likely indicates that the DNS server is either down or unreachable. | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| We were made aware of this incident at 1:24PM when several customers called to notify us that they could not get to our website. As soon as we were notified of the issue we attempted to get to the website ourselves and were also unable to reach the site.   We then turned on our network analyser and re-attempted to access the website. This showed the above error of “UDP port 53 unreachable”. Port 53 handles our DNS protocols, it being unreachable could be several things with the most likely being the DNS server itself is down.  Other possible causes could be a DDoS attack, configuration issue or error, or port 53 is blocked. |