# 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 down or unreachable  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: “UDP port 53 unreachable’’  The port noted in the error message is used for: Port 53 is commonly used for DNS protocol traffic. It is likely that the DNS server is not responding. | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| Time incident occurred: 1:24 mins and 32.192571 seconds in the afternoon  The IT team became aware of the incident: Several customers contacted the organization that they were not able to access the company’s website.  The actions taken by the IT department to investigate the incident: Network security team visited first the company’s website confirming about the incident. Next, the security team analyzed the problem in depth by loading the network analyzer protocol, which is tcpdump to see the incident in more detail.  Key findings of the IT department's investigation: After using the Network analyzer protocol, the network security team found out in the log file that DNS port 53 is unreachable.  Likely cause of the incident: Heavy network traffic, Wrong configuration of the firewall, or a successful Denial of Service is on going. |