# 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: port 53 is unreachable when attempting to access the website.  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 length 234  The port noted in the error message is used for: 53  The most likely issue is: The message is not going through to the DNS server. This may indicate a problem with the DNS servers. There may be an attack on the DNS server. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred: Occurred in the afternoon at 13:00 hours.  Explain how the IT team became aware of the incident: Customer complaints that mentioned access to the website was unavailable.  Explain the actions taken by the IT department to investigate the incident: The network security team responded and began running tests with the network protocol analyzer tool tcpdump.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): This means that the UDP protocol was used to request a domain name resolution using the address of the DNS server over port 53. The word “unreachable” in the message indicates the message did not go through to the DNS server.  Note a likely cause of the incident: DDoS attack on the DNS server or a firewall configuration blocking traffic on port 53. |