# 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 unreachable when users attempt to access the company 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.”**  The port noted in the error message is used for: **Port 53 is commonly used to** **request a domain name resolution using the address of the DNS server over the port. It is the port for DNS protocol traffic.**  The most likely issue is:  **It is likely a problem with the DNS server (server is not responding) or a possible malicious 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: **in the afternoon around 1:24 p.m.**  Explain how the IT team became aware of the incident: **Several customers contacted the company to report that they received the message: “destination port unreachable” when they attempted to access the company website.**  Explain the actions taken by the IT department to investigate the incident: **The IT security team responded and conducted packet sniffing tests using tcpdump. The resulting logs revealed that port 53, which is used for DNS protocol traffic is not reachable.**  **The next step is to identify whether the DNS server is down or traffic to port 53 is blocked by the firewall.**  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):  Note a likely cause of the incident: **A likely cause of the incident might be** **the DNS server is down due to a successful Denial of Service attack or port 53 is blocked by the firewall because of a misconfiguration.** |