# 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 company website www.yummyrecipesforme.com.  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: **udp port 53 unreacheable length 150**  Port 53 is the default port for DNS communication. DNS servers listen on this port for DNS queries and responses.  This may indicate a problem with the web server or the firewall configuration. It is possible that this is an indication of a malicious attack on the DNS server, as a DDoS. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| The incident occurred after lunch, around 13:24, when several customers reported that they were not able to access the company website, www.yummyrecipesforme.com, and saw the error "destination port unreachable" after waiting for the page to load. Several customers contacted your company to report that they were not able to access the company website, www.yummyrecipesforme.com, and saw the error "destination port unreachable" after waiting for the page to load. 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 the default port for DNS communication, is not reachable. We are continuing to investigate the root cause of the issue to determine how we can restore access to the secure web portal. 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. It is possible that this is an indication of a malicious attack on the DNS server, as a DDoS. |