# Cybersecurity Incident Report:

# Network Traffic Analysis

| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log. | |
| --- | --- |
| The network protocol analyzer logs reveal that TCP/UDP port 53 is inaccessible when users attempt to access yummyrecipesforme.com. Port 53 is typically used for Domain Name System (DNS) requests, which translate a domain name into the corresponding IP address of the website's server. This issue could point to a malfunction with the DNS server, misconfigured firewall settings, or problems during the TCP handshake process. Additionally, it might suggest a potential malicious attack targeting the web server. | |
|

| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| --- |
| The incident occurred today at 1:23 p.m. after customers reported error messages when attempting to access yummyrecipesforme.com. The error message displayed stated, “destination port unreachable.”  Using the network protocol analyzer tool, tcpdump, the cybersecurity analyst confirmed that UDP port 53, which handles DNS requests, is inaccessible. Attempts to retrieve the IP address for yummyrecipesforme.com via a UDP request resulted in an ICMP packet indicating that port 53 is unreachable. Investigations are ongoing to identify the root cause and restore site access.  Next steps include reviewing the firewall configuration to ensure port 53 hasn’t been inadvertently blocked and consulting the web server’s system administrator to check for potential signs of an attack.  Additionally, all TCP requests also return the same “port 53 unreachable” error, which may indicate the server is experiencing a Denial of Service (DoS) attack due to being overwhelmed with requests. The network security team is actively working on resolving the issue. |