# DoS: Cybersecurity Incident Report

|  |
| --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log |
| The network logs show that users are unable to access TCP/UDP port 53 when they try to visit yummyrecipesforme.com. Port 53 is typically used to communicate with the Domain Name System (DNS), which translates the website's name into the IP address of its server. This issue could be caused by a problem with the DNS server, firewall settings, or something going wrong during the process of connecting to the server. It's also possible that this might be part of a malicious attack on the server. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide one solution to implement |
| The incident happened today at 1:23 p.m., when customers reported error messages while trying to access yummyrecipesforme.com. They received a “destination port unreachable” error when visiting the site.  After analyzing the network using tcpdump, a cybersecurity analyst confirmed that UDP port 53, which handles DNS requests, is not accessible. Any attempt to request the IP address of yummyrecipesforme.com returns an error message (ICMP packet) indicating that port 53 is unreachable. The investigation is ongoing to find the cause and restore access to the site.  Next steps include reviewing the firewall settings to make sure port 53 isn’t blocked by mistake and contacting the server's system administrator to check for any signs of an attack.  All ICMP requests are also returning the same port 53 error, which could indicate a Denial of Service (DoS) attack. The network security team is continuing to work on fixing the issue. |