**Cybersecurity Incident Report**

|  |
| --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log |
| The network protocol analyzer logs show that TCP/UDP port 53 is unreachable when users try to visit yummyrecipesforme.com. Port 53 is normally used to request the Domain Name System (DNS) to convert a domain name into the IP address for the website’s server. This may indicate a problem with the DNS server itself, firewall configurations, or potentially there are issues occurring during the TCP handshake process. It is possible that this is an indication of a malicious attack on the web server. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide one solution to implement |
| The incident occurred today at 1:23 p.m. after customers called the organization to notify the IT team about error messages they were receiving when attempting to open the site yummyrecipesforme.com. The customers reported that they only see an error stating “destination port unreachable” when trying to visit the site.  After using the network protocol analyzer tool, tcpdump, the cybersecurity analyst has confirmed that UDP port 53 for DNS requests is not reachable. Making a UDP request for the IP address of yummyrecipesforme.com returns an ICMP packet stating that port 53 is unreachable. We are continuing to investigate to find the root cause for this issue so that we can restore access to the site.  Our next steps include checking the firewall configuration to ensure that port 53 wasn’t accidentally blocked and contacting the system administrator for the web server to check the system for signs of an attack.  All TCMP requests also return the error stating that port 53 is unreachable. This could suggest that the server is undergoing a Denial of Service (DoS) attack and is therefore overloaded with requests. The network security team will continue to find solutions to the outage. |