# Cybersecurity Incident Report:

# Network Traffic Analysis

|  |
| --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log |
| When the website [www.yummyreceipesforme.com](http://www.yummyreceipesforme.com) is accessed in tcpdump the error, “udp port 53 unreachable” Is displayed. In the error log the source Ip address was 192.51.100.15.5244, and the destination IP address was 203.0.113.2.domain and the IP address for the DNS server was 233.18.9.101.domain. The ICMP error message given for the destination IP indicates that the ICMP packet was undeliverable to the port of the DNS server. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide one solution to implement |
| Several customers contacted the 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. At 1:24 p.m. when tcpdump was loaded and tried to access the website the same error was received. This means that the UDP protocol was used to request a domain name resolution using the address of the DNS server over port 53. Port 53, which aligns to the .domain extension in 203.0.113.2.domain, is a well-known port for DNS service. The word “unreachable” in the message indicates the message did not go through to the DNS server. Your browser was not able to obtain the IP address for yummyrecipesforme.com, which it needs to access the website because no service was listening on the receiving DNS port as indicated by the ICMP error message “udp port 53 unreachable.” After the security analysts have figured out the issue it was forwarded to a supervisor who will task the security engineers to handle find a resolution. Hence, this could mean that there could be a port-filtering rule in the organizations firewall in which all network trying to access port 53 for the DNS lookup from external sources could be blocked. And the solution may be to review the prescribed port-filtering rules in the firewall and turn off that rule, and also to review other rules to see if they’re blocking traffic to any other domains. Or another plausible reason in why the DNS server is down could be due to a DoS attack. |