# Cybersecurity Incident Report:

# **Network Traffic Analysis Project**

You are a cybersecurity analyst working at a company that specializes in providing IT services for clients. Several customers of clients reported that they were not able to access the client company website www.yummyrecipesforme.com and saw the error “destination port unreachable” after waiting for the page to load.

You are tasked with analyzing the situation and determining which network protocol was affected during this incident. To start, you attempt to visit the website, and you also receive the error “destination port unreachable.” To troubleshoot the issue, you load your network analyzer tool, tcpdump, and attempt to load the webpage again. To load the webpage, your browser sends a query to a DNS server via the UDP protocol to retrieve the IP address for the website's domain name; this is part of the DNS protocol. Your browser then uses this IP address as the destination IP for sending an HTTPS request to the web server to display the webpage The analyzer shows that when you send UDP packets to the DNS server, you receive ICMP packets containing the error message: “udp port 53 unreachable.”



|  |
| --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log. |
| The network protocol analyzer logs indicates that port 53 is unreachable when attempting to send a UDP message requesting an IP address for the domain [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com) which did not go through to the DNS server because no service was listening on the receiving DNS port. The ICMP protocol was used to respond with an error indicating an issue with the DNS. Since port 53 is associated with DNS protocol traffic it means there’s a problem with the DNS server. The A? symbol indicates flags with performing DNS protocol operations.  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message about port 53, meaning the DNS server is not responding. I support my assumption by the flags associated with the outgoing UDP message and domain name retrieval. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| The incident occurred at 1:24 pm this afternoon when a user reported they were unable to load the yummy recipes website with the message “destination port unreachable”. The Network security team was immediately notified. The network security team then responded by conducting packet sniffing tests to analyze the issue using the network analyzer tool, tcpdump to resolve this issue to help the user gain access to this website as soon as possible.  The resulting logs show that port 53, which is used for DNS used to translate human readable domain names into IP addresses for computers to identify each other on the network was unreachable. Our next step is to whether the DNS server is down or traffic to port 53 is blocked by the firewall.  The security team is convinced that there could have been a possible DNS cache poisoning attack or a DDoS or the DNS server. |