# Cybersecurity Incident Report:

# Network Traffic Analysis

Review the scenario below. Then complete the step-by-step instructions.

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** |
| In the DNS protocol, UDP was utilized to communicate with the DNS server to retrieve the IP address for the domain name "yummyrecipesforme.com". Subsequently, an ICMP error message was received, signaling difficulties in contacting the DNS server. The log events illustrate the UDP message sent from the browser to the DNS server in the first two lines, while the ICMP error response from the DNS server to the browser, containing the error message "udp port 53 unreachable", is depicted in the third and fourth lines of each log event. The indication of "udp port 53 unreachable" suggests a problem with the DNS server since port 53 is designated for DNS protocol traffic. Further issues with DNS protocol execution are indicated by the presence of flags, including the plus sign after the query identification number 35084, denoting flags associated with the UDP message, and the "A?" symbol, indicating flags associated with DNS protocol operations. The ICMP error response message regarding port 53 strongly suggests unresponsiveness of the DNS server, a notion supported by the flags linked 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** |
| Today, at 1:24 p.m., the organization received reports from customers indicating they encountered the message "destination port unreachable" when attempting to visit the website yummyrecipesforme.com. The cybersecurity team, responsible for providing IT services to the organization, is presently investigating the issue to restore customer access to the website. As part of our inquiry, we conducted packet sniffing tests using tcpdump. Analysis of the resulting log file revealed that DNS port 53 was inaccessible. Our next course of action involves determining whether the DNS server is offline or if traffic to port 53 is blocked by the firewall. Potential causes for the DNS server being down include a successful Denial of Service attack or misconfiguration. |