**Cybersecurity Incident Report: Network Traffic Analysis**

|  |
| --- |
| **Part 1: Provide a summary of the problem found in the tcpdump log**  As part of the DNS protocol, the browser used the UDP protocol to query the DNS server for the IP address of `yummyrecipesforme.com`. However, the DNS server responded with an ICMP error, indicating a failure to establish contact. In the tcpdump logs, the outgoing UDP messages from the browser to the DNS server appear in the first two lines of each log event. The ICMP error responses — specifically stating “udp port 53 unreachable” — are shown in the third and fourth lines.  Since port 53 is designated for DNS traffic, this clearly points to a problem with the DNS server. The presence of DNS-related flags, such as the plus sign (`+`) following the query ID `35084` and the `"A?"` (indicating a request for an A record), further confirms that DNS resolution was attempted. Given the ICMP errors and the DNS-specific flags in the UDP request, it's highly likely that the DNS server is either down or not responding to queries. |
| **Part 2: Explain your analysis of the data and provide at least one cause of the incident.**  The incident occurred today at 1:24 p.m., when customers reported receiving a “destination port unreachable” error while attempting to access the website yummyrecipesforme.com. The cybersecurity team supporting the client organization promptly launched an investigation to restore access for users.  As part of the diagnostic process, we performed packet sniffing using tcpdump. The captured logs revealed that DNS traffic to port 53 was unreachable. This points to a potential issue with the DNS server. The next step is to determine whether the DNS server is down or if network traffic to port 53 is being blocked by a firewall. Possible causes include a successful Denial of Service (DoS) attack or a misconfiguration on the server. |