Cybersecurity Incident Report:

Network Traffic Analysis

|  |
| --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log. |
| The UDP protocol reveals that: when UDP packets are sent to the DNS server, client receives ICMP packets containing the error message: “udp port 53 unreachable.”  This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: “udp port 53 unreachable.”  The port noted in the error message is used for: Port 53 is a port for DNS service.  The most likely issue is:The word "unreachable" in the message indicates the UDP message requesting an IP address for the domain "[www.yummyrecipesforme.com](http://www.yummyrecipesforme.com/)" did not go through to the DNS server because no service was listening on the receiving DNS port. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred: The incident occurred in the afternoon at 13:24.  Explain how the IT team became aware of the incident: when several customers of clients reported that they were not able to access the client company website [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com/), and saw the error “destination port unreachable” after waiting for the page to load.  Explain the actions taken by the IT department to investigate the incident: IT department loaded network analyzer tool, tcpdump, and attempt to load the webpage again.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): To load the webpage, 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.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 the IT department sent UDP packets to the DNS server, they received ICMP packets containing the error message: “udp port 53 unreachable.”  Note a likely cause of the incident:The word "unreachable" in the message indicates the UDP message requesting an IP address for the domain "[www.yummyrecipesforme.com](http://www.yummyrecipesforme.com/)" did not go through to the DNS server because no service was listening on the receiving DNS port. |