Cybersecurity Incident Report:

Network Traffic Analysis

|  |
| --- |
| Part 1: Provide a summary of the problems found in the DNS and ICMP  traffic log. |
| The UDP protocol reveals that: destination port 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 requesting an IP address for the domain "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: 1:24 p.m., 32.192571 seconds  Explain how the IT team became aware of the incident: Several customers of clients reported that they were not able to access the client company website  Explain the actions taken by the IT department to investigate the incident:   1. Attempted to visit the website- Same result 2. Used Tcpdump and tried again 3. Query sent to DNS server via UDP protocol to retrieve IP address 4. Analyzer shows sent UDP packets to the DNS server, receiving ICMP packets containing the error message ‘UDP port 53 unreachable.”   Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):  With our investigation into the issue, we have found using Tcpdump that DNS Port 53 was unreachable. Our next step is to check to see if the DNS server is down or port 53 is blocked by the firewall. Also, the DNS server might be down to a successful DoS attack. |