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: attempted to send DNS requests to the server to the port 53 to connect to the  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: DNS  The most likely issue is: The DNS server 203.0.113.2 is down. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred: 13:24 and then 2 more attempts at 13:26 and 13:28  Explain how the IT team became aware of the incident: We noticed multiple failed attempts to connect on the tcpdump logs.  Explain the actions taken by the IT department to investigate the incident: Firewall may be blocking port 53 or the server is not running.  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): Impacted protocol is UDP, the impacted service is DNS port 53. All DNS requests failed to 203.0.113.2 for yummyrecipesforme.com . ICMP confirmed the DNS server port was closed/unavailable.  Note a likely cause of the incident: DNS service outage or misconfiguration. Could also be the target of a DoS/DDoS attack. |