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 it requested access to the website, it didn’t connect.  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: Communication about a connection error to the DNS server  The most likely issue is: The ICMP and DNS protocols are ineffective because they’ve been compromised due to connectivity issues. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred: 1:24 pm, then again at 1:26pm and last attempt was at 1:28pm  Explain how the IT team became aware of the incident: The customer complaints communicating their concerns to the company is how our IT team was able to get on it immediately.  Explain the actions taken by the IT department to investigate the incident:  The IT department confirmed the connectivity issues reported by customers about connecting to the company website, they loaded the Network Analyzer Tool, TCPDUMP and reloaded the website confirming more packets in the network analyzer. Lastly, it was confirmed that three attempts to connect to the website took place each resulting in “UDP port 53 unreachable”  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):  Note a likely cause of the incident: A likely cause of the incident could be an overflow of attempts to connect to the website all at once tied up the servers and temporarily or permanently crashed access to the website. |