Example of a

Cybersecurity Incident Report

|  |
| --- |
| **Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log** |
| The network protocol analyzer logs indicate that port 53 is unreachable when attempting to access the ‘yummyrecipcesforme’ website. Port 53 is normally used for Domain Name Resolution. This may indicate an issue with the network’s firewall configuration, but port 53 is also commonly subjected to DDoS attacks.  **\*edit –** While attempting to reach the yummyrecipesforme website, I was not able to and received an error message of “destination port unreachable”. Analyzing the logs from the network protocol analyzer, tcpdump, I see that the IP address attempts to connect with the DNS server but followed by an error log identification number 35084 and a plus sign indicating there’s flags associated with the UDP message and an “A?” which indicates a flag associates with the DNS request for a record which maps a domain name to the IP address. The the error message “udp port 53 is unreachable”. Port 53 is normally used for Domain Name Resolution. This indicates issues contacting the DNS server. The connectivity issue may be an issue with the network’s firewall configuration blocking port 53 or port 53 is commonly subjected to DDoS attacks. |
|

|  |
| --- |
| **Part 2: Explain your analysis of the data and provide at least one cause of the incident** |
| The incident was initially brought to attention as several customers trying to access the yummyrecipesforme.com received an error message “destination port unreachable”. Firstly, I tried to access the website but also received the error message. I then began running tests using the network analyzer tool, tcpdump. The resulting logs revealed that port 53, which is used for Domain Name Resolution, was not reachable. I am continuing to investigate the root cause of the issue to determine how we can restore access to the website. My steps include checking to see if in our firewall’s configuration is blocking port 53. Another issue it may be is that port 53 is commonly subjected to DDoS attacks. Some solutions is ensuring that the network’s firewall’s configurations enables port 53, implementing network ingress filtering, eliminating DNS resolvers, using random ports in place of port 53. |