Example of a

Cybersecurity Incident Report

This report **example** is for a different security event than the scenario presented in the activity. This example should only be used to familiarize yourself with the expected report format.

|  |
| --- |
| **Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log** |
| The port 53 of “yummyreceipesform.com” is unreachable when our users want to access the websites. Port 53 is normally used to ask the DNS the IP of the target website. This can be probably an ICMP Flood attempt. |
|

|  |
| --- |
| **Part 2: Explain your analysis of the data and provide at least one cause of the incident** |
| Several customers of clients reported that they were not able to access the client company website www.yummyrecipesforme.com and saw the error “destination port unreachable” after waiting for the page to load. Our cyber analyst launches a TCPDump protocol to understand what’s wrong and got the same issue. “ICMP 203.0.113.2 udp Port 53 is unreachable”. Our next step is to understand who is overloading the ICMP UDP Port 53 of the DNS server to restore the connection to the target website “yummyreceipesform.com”. The network security team suspects someone to send too big ICMP packet to the port 53 what make the port unreachable. |