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** | |
| --- | --- |
| Users couldn’t access www.yummyrecipesforme.com because the DNS service was unreachable. When the browser tried to ask the DNS server for the website’s IP address, it got an ICMP error: **“UDP port 53 unreachable.”** This means the DNS server was either down or blocked, preventing name resolution. Since DNS failed, the website couldn’t be loaded. | |
|

| **Part 2: Explain your analysis of the data and provide at least one cause of the incident** |
| --- |
| The data shows that the issue is with **DNS resolution over UDP**. The ICMP error “udp port 53 unreachable” confirms that the DNS server is not responding. Without DNS, the browser cannot find the website’s IP address, leading to the failure to load the site. |