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** | |
| --- | --- |
| Based on the log, we found that the UDP protocol reveals that the DNS server is down. 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”. It knows that port 53 is used for DNS protocol traffic. It can be concluded that the most likely issue is the DNS server not responding. | |
|

| **Part 2: Explain your analysis of the data and provide at least one cause of the incident** |
| --- |
| The incident occurred this afternoon when customer service contacted the IT department with a report from several customers stating the website cannot be accessed. The IT team tries to access the website and get an error “Destination host unreachable”. After that we run the network analyzer tool, tcpdump and catch error log “udp port 53 unreachable”. This indicate that we have problem with our DNS server and our professional team is undergoing further investigation |