Example of a

Cybersecurity Incident Report

|  |
| --- |
| **Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log** |
| Several customers contacted the company that they were not able to access the company website, [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com). As the team loaded the tcpdump and analyzed the data packet, the UDP protocol revealed that the DNS server was down and unreachable. If the ICMP shows an error message of ’’UDP port 53 unreachable’’, it is likely that the DNS server is not responding. |
|

|  |
| --- |
| **Part 2: Explain your analysis of the data and provide at least one cause of the incident** |
| The incident started around 1:24 p.m. To be exact, as shown in the data packet, around 1:24 minutes and 32.192571 seconds in the afternoon. Several customers contacted the organization about how they couldn’t access the company’s website, [www.yummyrecipesforme.com](http://www.yummtrecipesforme.com). The Network Security Department conducted an investigation into the said issue. The security team analyzed the situation to determine which network protocol was affected during the incident. First, the team visited the website and also received the error ‘’destination port unreachable''. After confirming the incident, the team loaded the network analyzer tool, specifically tcpdump. As a result, the team found out that DNS port 53 was unreachable, and ICMP packets sent two more logs indicating the same delivery error. The team is still doing the investigation and it is more likely that the DNS server is down, the firewall is configured incorrectly, or heavy traffic caused by a DDoS attack. |