Cybersecurity Incident Report:
Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.

The network analysis indicated that the UDP protocol was unable to reach port 53, which is used for both TCP and UDP communication in DNS servers. This was evident from the ICMP echo reply error message received during the network analysis, indicating that the ICMP packet was undeliverable to the DNS server's port 53. Given these findings, there was suspicion of a potential malicious attack, possibly an ICMP Flood Attack, targeting the web server.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.

On October 21, at 1:24 p.m. and 32.192571 seconds, a significant incident occurred where several customers reported being unable to access a company's website, receiving a "destination port unreachable" error. When the company investigated by visiting the website themselves, they encountered the same error. Using a network analyzer tool called tcpdump, they reloaded the webpage and observed a significant influx of packets. Analysis of these packets revealed that when UDP packets were sent to the DNS server's address over port 53, the response received was an ICMP error message indicating that UDP port 53 was unreachable. UDP port 53 is the well-known port for DNS service, suggesting a failure in the DNS resolution process. This situation raised concerns about a potential malicious attack, possibly an ICMP Flood Attack, targeting the web server.

-Kushagra Gupta