Cybersecurity Incident Report: Network Traffic Analysis

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

The analysis of the DNS and ICMP traffic log has identified a problem. Specifically, the UDP protocol has indicated that the destination port is unreachable. This issue is confirmed by the ICMP echo reply, which contains an error message stating that udp port 53 was unreachable. Port 53 is commonly associated with DNS (Domain Name System) communication.

Given these findings, the most probable cause of the problem is suspected to be a distributed denial-of-service (DDoS) attack. DDoS attacks aim to overwhelm a network or system with a high volume of traffic, leading to service disruptions. In this case, the attack appears to be targeting the DNS service by rendering port 53 unreachable. Further investigation and appropriate countermeasures are recommended to address and mitigate this potential DDoS attack.

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

Upon analyzing the data, a significant incident emerged in the network. The UDP protocol indicated an issue with the destination port, specifically port 53, which was found to be unreachable. This finding was corroborated by the ICMP echo reply containing the error message "udp port 53 was unreachable." The incident occurred precisely at 1:23 pm.

Awareness of the incident was prompted by reports from customers who were facing service disruptions. This triggered a swift response from the IT team to investigate and address the situation.

For the investigation, the IT department leveraged the tcpdump packet analyzer. This tool facilitated the capturing and analysis of network packets, enabling insights into the abnormal network behavior.

Key findings from the investigation centered on the affected port, port 53, commonly associated with DNS services. The DNS server emerged as a focal point within the incident.

Considering the gathered evidence, the incident's likely cause points toward a distributed denial-of-service (DDoS) attack. DDoS attacks involve overwhelming a target with excessive traffic to render it unreachable, causing service disruptions. In this scenario, the DDoS attack may have targeted the DNS service by inundating port 53.

In response, the IT team's investigation equips them with essential insights to address the incident's implications and implement measures to mitigate the impact of the DDoS attack.