Security Incident Report:
Network Traffic Analysis

Part 1: Summary of the problem found in the DNS and ICMP traffic log.
The “tcpdump” logs indicate an inability to reach UDP Port 53 when customers or employees attempt website access. Port 53 serves as the standard for both TCP and UDP communications, crucial for DNS operations. DNS client applications rely on this port to query DNS servers and receive information back. This issue may stem from firewall configuration errors or unresponsive behavior from the DNS server.

Part 2: Analysis of the data and causes of the incident.
At 1:24 p.m. precisely, the IT support team encountered a surge in customer complaints regarding website inaccessibility, accompanied by "destination port unreachable" error messages. To delve deeper into the matter, the Network Security team initiated packet sniffing tests on the website using "tcpdump" for a comprehensive investigation. Analysis of the logs revealed the unreachability of port 53, the standard DNS port. This issue appears linked to potential misconfigurations within the firewall or a plausible scenario of a DoS attack resulting in DNS server instability.