Cybersecurity Incident Report:
Network Traffic Analysis

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

The UDP protocol reveals that: Requests to communicate with the DNS server are returning unsuccessful. The TPS Handshake could not be completed as requested. The DNS server has temporarily crashed. Business Continuity has been breached due to an ongoing attack. Data may be compromised and/or lost due to the crash.

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”.

The port noted in the error message is used for: Port (53) is used for the DNS service. Translating the Domain Name into the corresponding IP address.

The most likely issue is: A Network Level DoS ICMP Flood Attack designed to clog our Network Bandwidth.

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

Time incident occurred: 13:24:32.192571 (approximately 1:24p.m.)

Explain how the IT team became aware of the incident: The IT team received reports from several customers claiming to not be able to reach our website. Instead a “udp port 53 unreachable” error message would be displayed across their web browser. We chose to follow up.

Explain the actions taken by the IT department to investigate the incident: We conducted a Network Traffic Analysis by testing the network with trial requests using a command line based Network Protocol Analyzer and sending UDP packets to the alleged affected port. Once multiple requests came back unsuccessful, we determined that the likely Cause of the incident is an ICMP Flood Attack.

Note a likely cause of the incident: ICMP Flood Attack. A possible path to resolve the issue would be to recall the point in time the first incident was reported, locate the source IP address by tracking the attack and then blocking any further requests from the source IP address by updating the configuration of an existing firewall.