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: the request for domain name resolution using the address of the DNS server over port 53 was unsuccessful because the message did not reach the DNS server. DNS server unreachable

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: DNS service/DNS protocol traffic.

The most likely issue is: The DNS server is not responding, possibly due to a SYN flood attack making port 53 unavailable.

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

Time incident occurred: 13:24

Explain how the IT team became aware of the incident: Several customers contacted the company to report that they were not able to access the company website and saw the error "destination port unreachable" after waiting for the page to load.

Explain the actions taken by the IT department to investigate the incident: The IT department responded by visiting the website, where they received the same error reported by customers. The IT department then began running tests with tcpdump and analyzed the tcpdump output.

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): The resulting logs revealed that the ICMP packet was undeliverable to the port of the DNS server when the UDP protocol was used to request a domain name resolution using the address of the DNS server over port 53. Found that DNS port 53 is unreachable.

Note a likely cause of the incident: A SYN flood attack might be making the DNS server's port unreachable. DNS server could be down or traffic to port 53 could be blocked by firewall; causes of DNS server being down could be DoS attack or misconfiguration.