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: ICMP packet was undeliverable to the port of the DNS server

This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: UDP port 53 is unreachable

The port noted in the error message is used for: to request a domain name resolution using the address of the DNS server

The most likely issue is: this is an indication of a malicious attack on the web server

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

Time incident occurred: 1:24 PM

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 team started running tests using network protocol analyzer tool tcpdump

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): IT found out that the UDP port 53 was unreacheable, which is used to request domain name resolution using the address of DNS server.
Note a likely cause of the incident: a possible DoS attack by a threat actor