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: It couldn't connect to port 53 on the DNS server to finish the handshake protocol (TCP/IP protocol) to upload the website. This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: UDP port 53 (on the DNS server) is unreachable. The port noted in the error message is used for: DNS services, meaning that the request to the website couldn't reach the DNS server hosting the website IP address. The most likely issue is: A SYNS attack because it dealt with the DNS server and handshake protocol, which can mean its likely a DoS attack.

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

Time incident occurred:
At 1:24 pm

Explain how the IT team became aware of the incident:
They became aware after several customers of clients had reported not gaining access to the website and getting “destination report unreachable” errors.

Explain the actions taken by the IT department to investigate the incident:
We first attempted to visit the website and got the same response as the customers. Then we began troubleshooting by querying the DNS server to reload the website with the network analyzer tool tcpdump. The response was a plus sign after the query ID number meant it was flagged as associated with the UDP level. The flag “A?” meant a DNS request but was returned with an ICMP error “UDP port 53 unreachable”. Port 53 is used for DNS services, so for it to be unreachable means that the DNS server is unavailable and most likely overloaded with requests.

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):

- The DNS server was unreachable, (port 53 unreachable)

Note a likely cause of the incident:
The most likely cause of this incident is a DoS attack on the DNS server. Could be targeting the client website or another website IP address stored on the server.