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: **DNS query goes out via UDP from user IP to DNS Server at 203.0.113.2** This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: **and receives ICMP "udp port 53 unreachable"** The port noted in the error message is used for: **Port 53** The most likely issue is: **UDP port 53 is either closed or blocked. Destination host is either actively rejecting the connection, is blocked by firewall, or the DNS service is not running on that port.**

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: **Approx 13:24** Explain how the IT team became aware of the incident: **Multiple users reported unable to access client's website** Explain the actions taken by the IT department to investigate the incident: • **IT analyst accessed the website and received same error** • **Analyst used tcpdump to monitor network traffic while attempting connection** • **Analyst analyzes the packet captures to determine the issue** • **Analyst observes that DNS queries sent to DNS resulted in port unreachable** Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): • DNS server's IP is 203.0.113.2 • All DNS queries were sent over UDP port 53 (standard DNS port) • Port 53 unreachable

- Because DNS resolution failed, the web browser couldn't get the IP address for the website the client is attempting to access

Note a likely cause of the incident:

- DNS service down
- Firewall rule blocking UDP traffic
- Misconfiguration on the DNS server preventing it from listening on port 53