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 DNS query sent using UDP could not reach 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 unreachable

The port noted in the error message is used for: DNS services (UDP port 53 is used to send domain name queries).

The most likely issue is: The DNS server is down or not responding on port 53, causing domain resolution to fail.

A DNS query was sent this morning using UDP which could not reach the DNS server. Based on the results of the network analysis, UDP port 53 shows unreachable and the ICMP echo reply returned to the error message. The port noted in the error message is used for DNS services (used to send domain name queries).The most likely issue is that the DNS server is down or not responding on port 53, causing domain resolution to fail.

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

Time incident occurred: Between 13:24:32 and 13:28:50, as per the tcpdump log timestamps.

Explain how the IT team became aware of the incident: Multiple customers reported being unable to access the website and received a “destination port unreachable” error.

Explain the actions taken by the IT department to investigate the incident: The team used tcpdump to monitor DNS traffic and discovered repeated ICMP error messages indicating that DNS requests were not being fulfilled.

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): UDP DNS requests to IP 203.0.113.2 on port 53 were not received. ICMP replies indicated that the DNS server was not listening or available at that port.

Note a likely cause of the incident: The DNS server (or service on port 53) may have crashed, been misconfigured, or blocked by a firewall.

The incident occurred this morning when multiple customers reported being unable to access the website and received a “destination port unreachable” error. The team became aware of it when multiple errors were reported. The team used tcpdump to monitor DNS traffic and discovered ICMP error message indicating the DNS message were not fulfilled. The key findings of the IT department are the UDP request was sent at 1:24pm in the afternoon to 203.0,112.2 on port 53 were not received. ICMP replies indicated that the DNS servers were not listening or available at that port. The most likely cause of the incident is the DNS server or service port 53 may have crashed, been misconfigured, or blocked by a firewall.