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: there is a flag associated with the UDP message from the "+" sign after the query identification number 35084. We also know that there is a flag associated with the DNS request for an A record, where an A record maps a domain name to an IP address from the "A?". 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 The most likely issue is: UDP message requesting an IP address for the domain website did not go through to the DNS server because no service was listening on the receiving DNS port from the word "unreachable". **The network protocol, UDP protocol, reveals that there is a flag associated with the UDP message from the "+". It also reveals that there is a flag associated with the DNS request for an A record, where an A record maps a domain name to an IP address from the "A?". The ICMP echo reply returned the error message "udp port 53 unreachable", which indicates that port 53 is unreachable when attempting to access the company's domain website. Port 53 is normally used for DNS services. This may indicate a problem with the DNS server since no server was listening on the receiving end of the DNS port for the IP address for the domain website.**

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: The outgoing request happened at 1:24 PM 32.192571 seconds in, 1:26pm 32.192571 seconds in, and 1:28pm 32.192571 seconds in. The response happened at 1:24PM 36.098564 seconds in, 1:27PM 15.934126 seconds in, and 1:28PM 50.022967 seconds in. Explain how the IT team became aware of the incident: Several customers of clients were

not able to access the client 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: Attempted to visit the website and also received the error. Loaded network analyzer tool, tcpdump, and attempted to load the webpage again. Got an error message saying “udp port 53 unreachable” from the tcpdump log.

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): Request for an IP address for the domain did not go through to the DNS server since no service was listening on the receiving DNS port.

Note a likely cause of the incident: Problem with the DNS server since it could not do its job where it translates internet domain names into IP addresses. Could not fetch the IP address for the HTTPS so it could not display the webpage. Could be an attack for the DNS server or port 53 is closed.

This incident occurred around 1:24PM when multiple clients were having trouble accessing the client company’s website and saw the error “destination port unreachable” after waiting for the page to load. The IT department took action by attempting to visit the website and loading network analyzer tool, tcpdump, and attempted to load the webpage again. The tcpdump revealed that port 53, which is used for DNS servers, is not reachable. We are continuing to investigate the root cause of the issue to determine how we can restore access to the company’s website. Our next steps include checking the firewall configuration to see if port 53 is blocked, checking if the DNS server is down or look for signs of an attack.