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: UDP packet was undeliverable to port 53 of the DNS Server which is used for DNS queries 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. This means that the DNS server did not respond to the DNS request because port 53 was not accessible, indicating no service was available to handle the DNS request. The port noted in the error message is used for: Port 53 is used for DNS queries, which is responsible for translating domain names to IP addresses that direct traffic to the correct web servers The most likely issue is: either the server is down or misconfigured, or Denial of Service attack on the DNS server because it prevents the users from accessing the website The network protocol analyzer logs indicate that port 53 is unreachable when attempting to access the client company www.yummyrecipesforme.com website. Port 53 is normally used for DNS queries. This may indicate a problem with translating domain names to IP addresses that direct traffic to the correct web servers. It is possible that this is an indication that the server is down or misconfigured or a Denial of Service attack on the DNS server because it prevents the users from accessing the website.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: 1:24pm 32.192571 seconds Explain how the IT team became aware of the incident: Several customers of clients reported that they were not able to access the client company website www.yummyrecipesforme.com, 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 network security team responded and began attempting to visit the website, run the network

protocol analyzer tool tcpdump, load the webpage again, and check the new traffic in tcpdump.

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

- The DNS server at **IP address 203.0.113.2** was not responding to DNS requests because port 53 was unavailable.
- The error **"udp port 53 unreachable"** suggests that the DNS service was not running or misconfigured on the server.
- The server responded with ICMP packets indicating that the **UDP packets** sent to port 53 could not be processed.

Note a likely cause of the incident: The **DNS service** on the server became unavailable due to either a **service failure**, **server misconfiguration**, or possibly a **DDoS attack** targeting the DNS server, rendering it unable to handle requests on port 53. Another possibility is that a network misconfiguration blocked access to port 53, preventing it from responding to UDP requests.

The incident occurred in the afternoon around 1:24pm 32.192571 seconds when several customers of clients reported that they were not able to access the client company website www.yummyrecipesforme.com, and saw the error "destination port unreachable" after waiting for the page to load. The network security team responded and began attempting to visit the website, run the network protocol analyzer tool tcpdump, load the webpage again, and check the new traffic in tcpdump. The resulting logs revealed that port 53, which is used for DNS Server traffic, is not reachable. We are continuing to investigate the root cause of the issue to determine how we can restore access to a secure web page. Our next steps include checking the firewall configuration to see if port 53 is blocked and contacting the system administrator for the web server to have them check the system for signs of an attack.