Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
The UDP packets were sent from the client's computer to the DNS server to request the IP address of www.yummyrecipesforme.com but was not reachable. 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 tcpdump log analysis reveals repeated occurrences of port 53, commonly associated with DNS traffic. The primary protocols observed are UDP and ICMP. The port noted in the error message is used for: Port 53, which is used for DNS (Domain Name System) service. The log indicates that the DNS server on port 53 is unreachable, stopping any successful resolution of the domain www.yummyrecipesforme.com. The issue is with the DNS server.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident occurred at 13:24:32.192571 (1:24 p.m.), indicating the exact time of the issue. Several customers reported being unable to access the client company website www.yummyrecipesforme.com, receiving the error "destination port unreachable." The IT team became aware when the cybersecurity analyst attempted to visit the website and encountered the same error. The IT department used a network analyzer tool, tcpdump, to capture and analyze network traffic during the incident. This involved sending UDP packets to the DNS server to retrieve the IP address for the website's domain name. key findings of the IT department's investigation: Source IP: 192.51.100.15 (client's computer) Destination IP: 203.0.113.2 (DNS server) Destination Port: 53 (DNS service) Protocol: UDP (DNS request) and ICMP (error response) Error Message: "udp port 53 unreachable" Additional Details: + sign indicated flags associated with the UDP message. query identification number: 35084 . "A?" indicates a flag associated with the DNS request for an A record. The most likely cause is a failure in communication between the client's computer and the

DNS server on port 53. Potential causes include firewall-blocking UDP traffic, DNS server issues, network connectivity problems, or DNS spoofing/hijacking.

Next Steps in Troubleshooting and Resolving the Issue:
a. Verify firewall settings.
b. Check the DNS server for issues.
c. Investigate network connectivity problems.
d. Examine the possibility of DNS spoofing/hijacking attempts.