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 browser sends a DNS query using UDP to port 53 to retrieve the IP for "yummyrecipesforme.com."

This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: The response indicates “udp port 53 unreachable,” meaning the DNS server did not process the request.

The port noted in the error message is used for: Port 53, which is used for DNS services.

The most likely issue is:The DNS service on port 53 is not available or there’s a misconfiguration preventing the request from reaching the DNS server.

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

Time incident occurred:13:24:32.192571.

Explain how the IT team became aware of the incident:Customers reported being unable to access the website and receiving a "destination port unreachable" error.

Explain the actions taken by the IT department to investigate the incident:The IT department captured network traffic using tcpdump and discovered ICMP error messages indicating UDP traffic to port 53 was blocked or unreachable.

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): UDP packets were sent from the browser to DNS, but ICMP replies showed port 53 was unreachable. The DNS server at IP 203.0.113.2 did not process the DNS request.

Note a likely cause of the incident:The DNS server’s service may have been down or misconfigured, causing port 53 to be unavailable.