Trent Dozier

Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
The network analyzer logs indicate that an error is occurring at the transport layer as noted from the UDP protocol error. The port noted in the error is 53 which is used for DNS lookup requests. The ICMP echo reply returned the error message “UDP port 53 unreachable”. The most likely issue is that the request to resolve the website address did not go through because no service was listening on the receiving DNS port. The log also shows two more attempts were made with the same error message.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident occurred at 1:24pm and we were made aware of the issue by a client trying to reach yummyrecipes.com but they were not able to get through. For the ICMP error repose the source address is 203.0.113.2. There are flags associated with the DNS request for an A record. Possible causes could be an issue with the DNS record on this domain, being blocked by a firewall or a DOS attack on the DNS server.