Junaid shakoor
Cybersecurity incident report network traffic analysis
7/25/2024
shakoor.junaidre@gmail.com

Part 1: Summary of the Problem

The network protocol analyzer logged that the destination port is unreachable. The error code "udp port 53 unreachable" indicates a problem with DNS (Domain Name System) service. The DNS server, which is responsible for translating domain names into IP addresses, is either not responding or cannot be accessed.

Part 2: Analysis and Potential Cause

The incident occurred at 1:24 PM and 32.192571 seconds. The IT department was alerted when numerous customers reported being unable to access the website "yummyrecipesforme.com" and received the error "destination port unreachable."

A security specialist attempted to access the website with a regular browser and encountered the same error. To troubleshoot, the network analyzer tool, tcpdump, was used to examine the network traffic while trying to load the website.

The tcpdump log reveals multiple failed attempts to contact the DNS server at IP address 203.0.113.2 on port 53. This confirms that the DNS service was not functioning or accessible during the incident.

A possible cause of the incident is that the DNS server at 203.0.113.2 may be experiencing an outage, is misconfigured, or is under a denial-of-service (DoS) attack.