Cybersecurity Incident Report: Network Traffic Analysis

Summary

The TCPDump log shows that the UDP protocol was used to contact the DNS server in order to retrieve the IP address for the domain yummyrecipesforme.com, as part of the normal DNS lookup process. However, the ICMP protocol responded with an error message indicating a problem contacting the DNS server.

In each log event, the first two lines show the UDP request from the browser to the DNS server, and the third and fourth lines show the ICMP error response from the DNS server back to the browser, containing the message “udp port 53 unreachable.” Because port 53 is associated with DNS traffic, this indicates an issue specifically related to the DNS server.

Additional indicators, such as the plus sign following the query identification number 35084 and the “A?” symbol, confirm that the UDP message and DNS query encountered errors. These flags, combined with the ICMP “port unreachable” message, strongly suggest that the DNS server is not responding to requests.

Analysis

The incident occurred today at **1:24 p.m.**, when customers reported receiving the message **“destination port unreachable”** while attempting to visit *yummyrecipesforme.com*. The cybersecurity team began investigating to restore website access.

Packet analysis using **tcpdump** revealed that **DNS port 53** was unreachable. This finding suggests that the DNS server is either **down** or **blocked by a firewall**. The root cause could be one of the following:

- The DNS server may have become **unavailable due to a Denial of Service (DoS) attack**, overwhelming its resources.
  A **firewall misconfiguration** could be blocking DNS traffic on port 53, preventing successful name resolution.

Further investigation is required to determine whether the DNS server is offline or if network security settings are restricting DNS traffic.