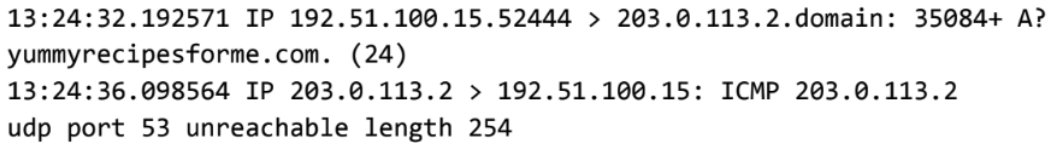
Cybersecurity Incident Report:
Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.

The UDP protocol reveals that: There is an error

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 length 254

The port noted in the error message is used for: DNS domain name resolution
This means that the UDP protocol was used to request a domain name resolution using the address of the DNS server over port 53.
The most likely issue is that no service was listening on the receiving DNS port as indicated by the ICMP error message “udp port 53 unreachable as indicated by the tdcpumb



```
13:24:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:24:36.098564 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 254
```

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

Time incident occurred: 13:24:32.192571 in log but several costumer reported this issues
So the time of the incident can be determinate to be prior the first console log
Becuase several customers contacted our company to report that they were not able to access our company website www.yummyrecipesforme.com, and saw the error “destination port unreachable” after waiting for the page to load.
I started taking action to investigate the incident Once I captured the data packets using a network analyzer tool, I identify which network protocol and service were impacted by this incident. Then, i will need to write a follow-up report. As an analyst, I can inspect network traffic and network data to determine what is causing network-related issues during cybersecurity incidents.
Our next steps include checking the firewall configuration to see if port 443 is blocked and contacting the system administrator for the web server to have them check the system for signs of an attack.
The word “unreachable” in the message indicates the message did not go through to the DNS server. Your browser was not able to obtain the IP address for yummyrecipesforme.com, which it needs to access the website because no service was listening on the receiving DNS port as indicated by the ICMP error message “udp port 53 unreachable.”

Luca Forma