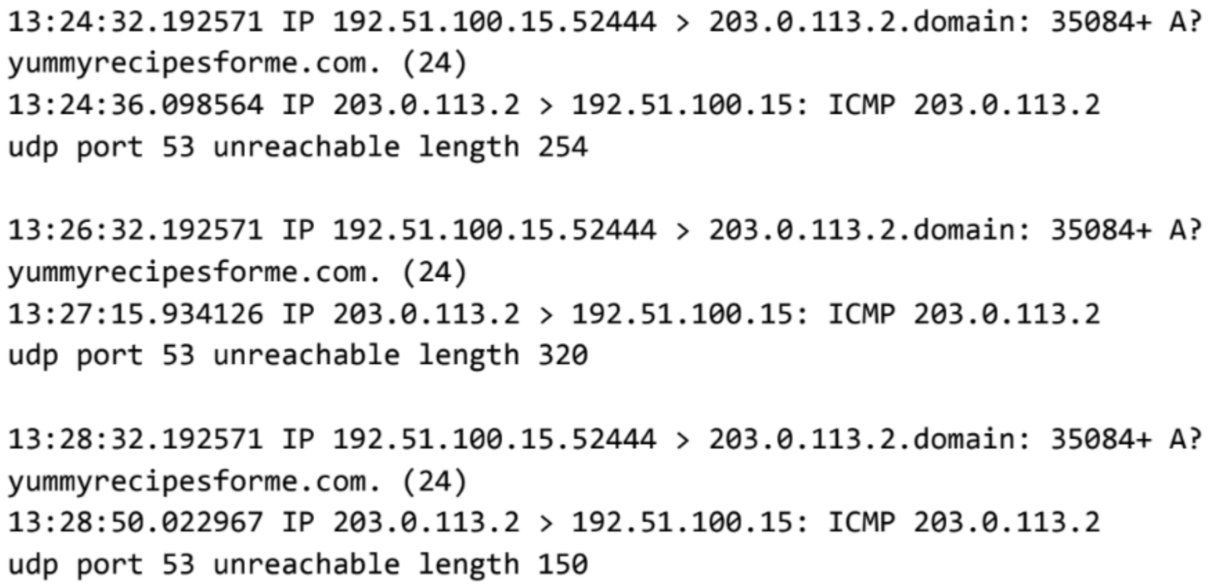
Summary

After analyzing the data presented from the tcpdump log, there was a trend found in the data. The tcpdump log starts at 13:24 and ends at 13:28 meaning that it tried to reach its destination via DNS 3 times which resulted in port 53 being unreachable. The query number 35084+ A also shows issues with the DNS and protocols. Furthermore, the ICMP error response message regarding port 53 supports that the DNS server is not responding. Due to that error, the assumption is hard to ignore when the flags are with the outgoing UDP message and domain name retrieval. As of right now, the network protocol (UDP/TCP) has been identified as the incident.

Currently, the event is being handled by security engineers after and other analysts have reported the issue to higher-up individuals. However, the UDP network layer protocol has identified that there is a problem with the DSP issuing a udp port 53 unreachable meaning that tcp log is identifying packets into the terminals without a response. These attacks can be very damaging to an organization. Therefore I recommend a coupe of things be done, check for updates, restart-reset-restore, uninstall and reinstall, 3rd party filtering, implement network filtering as well as other suggestions can be made. However, our special team of supervisors has started working on the problem right now.



```
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

13:26:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:27:15.934126 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 320

13:28:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:28:50.022967 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 150
```

Step 3: Provide a summary of the problem found in the tcpdump log

Identify trends in the data. Assess which protocol is producing the error message from the DNS server for the yummyrecipesforme.com website. Recall that one of the ports that is displayed repeatedly is port 53, commonly used for DNS.

In your analysis:

- Include a brief summary of the tcpdump log analysis and identify which protocols were used for the network traffic.
- Provide a few details about what was indicated in the log.
- Interpret the issues found in the log.

Record your responses in part one of the cybersecurity incident report.

Step 4: Explain your analysis of the data and provide one solution to implement

Now that you've inspected the traffic log and identified trends in the traffic, describe why the error messages appeared on the log. Use your answer in the previous step and the scenario to identify the reason behind the ICMP error messages. The error messages indicate that there is an issue with a specific port. What do the different protocols involved in the log reveal about the incident? In your response:

- State when the problem was first reported.
- Provide the scenario, events, and symptoms identified when the event was first reported.
- Explain the current status of the issue.
- Describe the information discovered while investigating the issue up to this point.
- List the next steps in troubleshooting and resolving the issue.
- Provide the suspected root cause of the problem.

Record your responses in part two of the cybersecurity incident report.