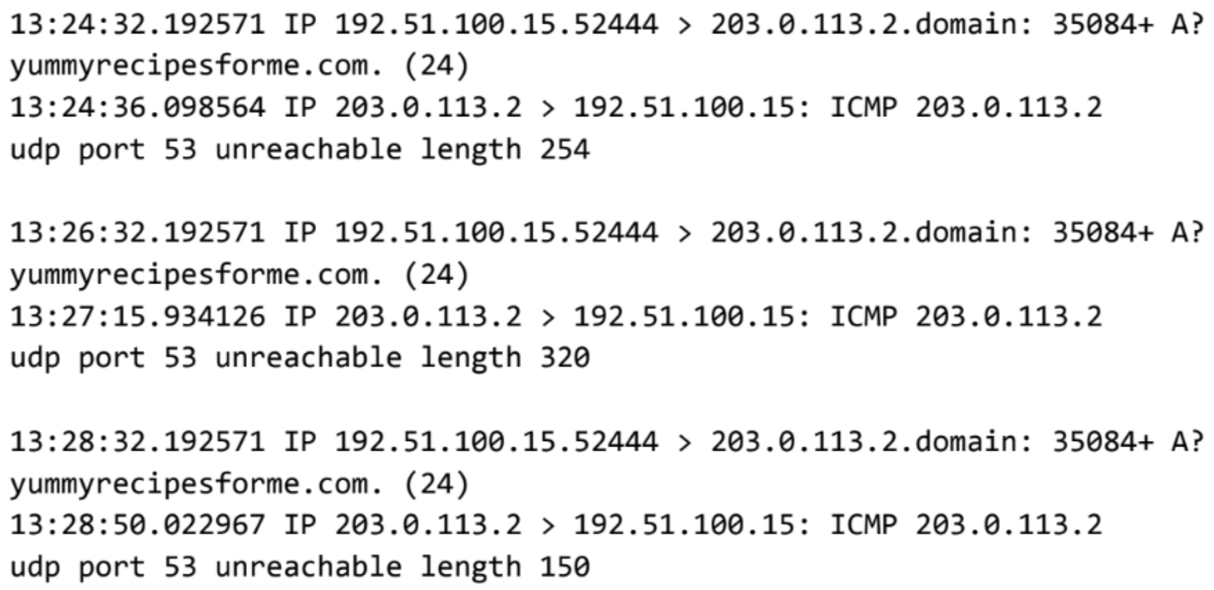
Case Study:

Analyze Network Layer Communication - Incident Reporting

Scenario:

You are a cybersecurity analyst working at a company that specializes in providing IT consultant services. Several customers contacted your company to report that they were not able to access the company website www.yummyrecipesforme.com, and saw the error “destination port unreachable” after waiting for the page to load.

You are tasked with analyzing the situation and determining which network protocol was affected during this incident. To start, you visit the website and you also receive the error “destination port unreachable.” Next, you load your network analyzer tool, tcpdump, and load the webpage again. This time, you receive a lot of packets in your network analyzer. The analyzer shows that when you send UDP packets and receive an ICMP response returned to your host, the results contain an error message: “udp port 53 unreachable.”



```
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
```

Now that you have captured data packets using a network analyzer tool, it is your job to identify which network protocol and service were impacted by this incident. Then, you will need to write a follow-up report.

As an analyst, you can inspect network traffic and network data to determine what is causing network-related issues during cybersecurity incidents.

Incident Report

Tcpdump Results

The first sequence of numbers displayed in the log are the timestamps which follow the format of *hour:minute:seconds*. In the first ICMP packet, this number is 13:24:32.192571

The next sequence of numbers displayed in the log which follow IP and end at the greater than symbol (>) refer to the IP address of the source. In this case, that would be my computer's IP address: 192.51.100.15.52444

The next sequence of numbers displayed in the log after the greater than symbol (>) and end at the colon symbol (:) refer to the IP address of the destination. In this case, that would be the DNS server's IP address: 203.0.113.2.domain

The second and third lines of the log begins with another timestamp and displays the response of the first ICMP packet.

The message "udp port 53 unreachable" refers to which protocol was used to handle communications and which port it was delivered to. In this case, the UDP protocol was used to request a domain name resolution using the address of the DNS server, which is commonly over port 53. The word "unreachable" indicates the message did not go through.

The remaining lines in the log indicate that ICMP packets were sent two more times but received the same error message.

Due to this, the browser was unable to obtain the IP address for yummyrecipesforme.com, which it needs to access the website.

Therefore, the results of the tcpdump show that the DNS server on port 53 is either down or unreachable.

Summary and Next Step

The results of the network analyzer tool, tcpdump, resulted in the ICMP echo reply "udp port 53 unreachable." Since port 53 is commonly used for DNS protocol traffic, it is highly likely that the DNS server is either down or unreachable.

The next step is to determine why the DNS server is down or unreachable. Possible causes can be a misconfiguration in the firewall blocking port 53 or a successful Denial of Service (DoS) attack.