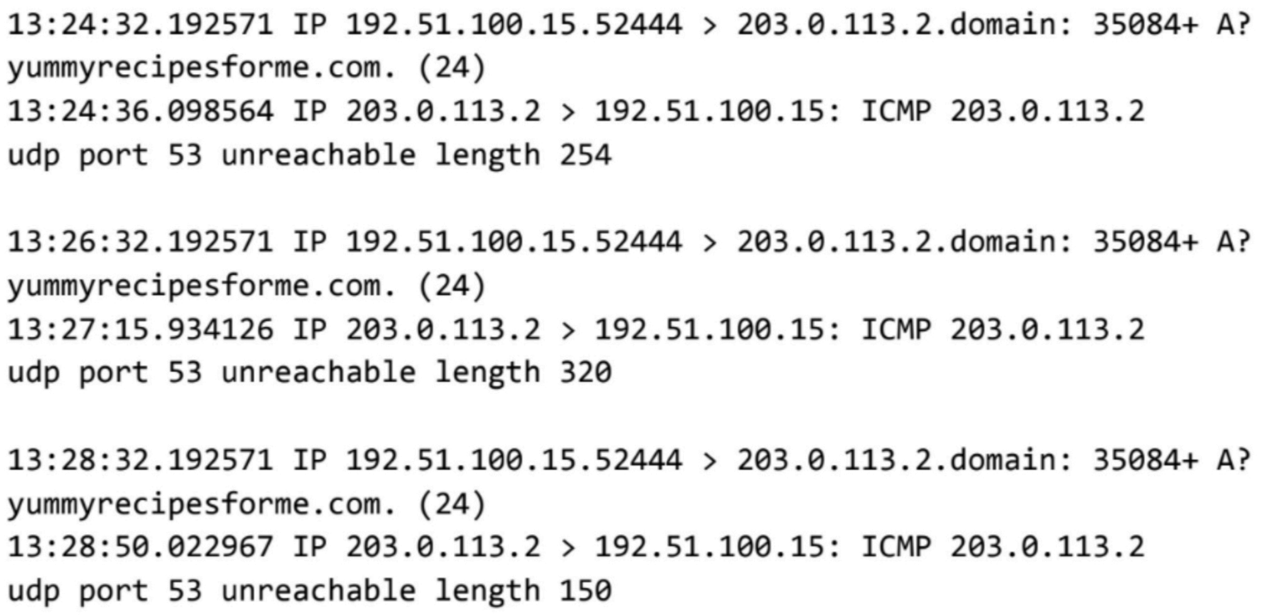
Scenario

Review the scenario below. Then complete the step-by-step instructions.

You are a cybersecurity analyst working at a company that specializes in providing IT services for clients. Several customers of clients reported that they were not able to access the client 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 attempt to visit the website and you also receive the error “destination port unreachable.” To troubleshoot the issue, you load your network analyzer tool, tcpdump, and attempt to load the webpage again. To load the webpage, your browser sends a query to a DNS server via the UDP protocol to retrieve the IP address for the website's domain name; this is part of the DNS protocol. Your browser then uses this IP address as the destination IP for sending an HTTPS request to the web server to display the webpage The analyzer shows that when you send UDP packets to the DNS server, you receive ICMP packets containing the 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
```

Cybersecurity Incident Report
(Network Traffic Analysis)

Incident ID: YR-2024-001

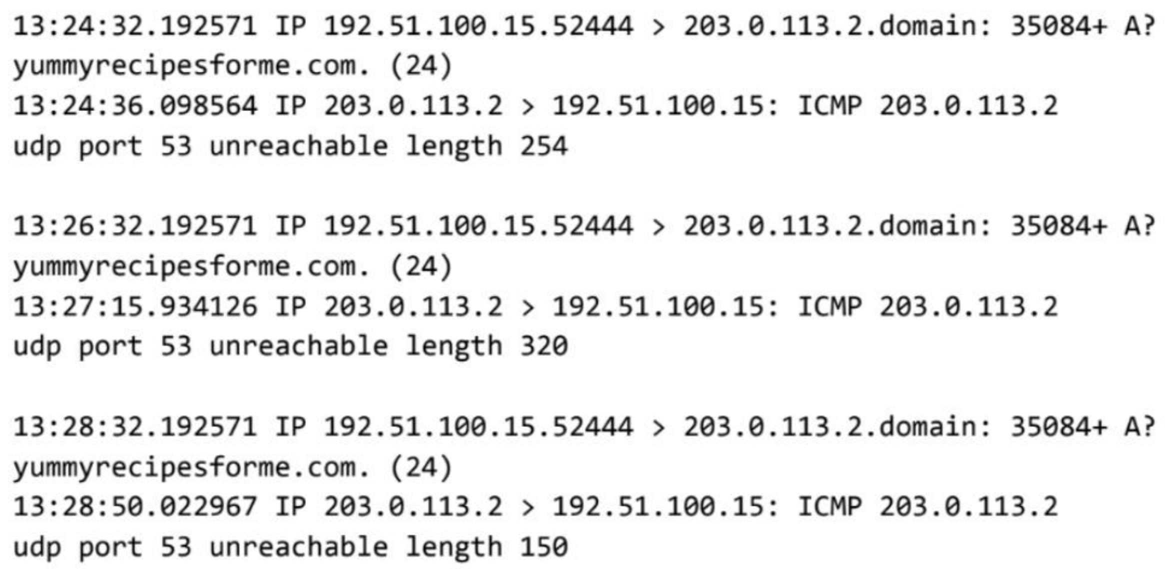
Reported by: Love

Date of Incident: 13:24:32 on 12/11/2024

Date of Report: 12/11/2024

Appendices :

Analysis Tool: tcpdump logs showing the DNS requests and ICMP responses for verification.



```
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
```

Part 1: Summary of the problem found in the DNS and ICMP traffic log

The network protocol analyzer logs indicate that port 53, which is used for DNS traffic, is unreachable when attempting to resolve the domain www.yummyrecipesforme.com.

DNS resolution is a critical function that allows clients to translate domain names into IP addresses. The unreachability of port 53 on the DNS server suggests an issue with the DNS configuration or network setup, which may be causing disruptions in accessing the requested website.

The log entries show ICMP "destination port unreachable" messages, indicating that the DNS server may not be properly configured to respond to requests or there may be a firewall or network policy blocking DNS traffic.

While there is no evidence at this time to suggest malicious intent, the lack of DNS resolution effectively prevents access to the site.

Part 2: Analysis of the Data and Possible Causes of the Incident

The incident was reported when users were unable to access www.yummyrecipesforme.com and encountered errors indicating that the destination was unreachable. Upon investigation using the tcpdump tool, it was found that the DNS server at IP address 203.0.113.2 was not responding to DNS queries sent from the client IP 192.51.100.15. This resulted in a series of ICMP "udp port 53 unreachable" messages being returned from the DNS server, which confirms that the DNS queries were unsuccessful.

Possible Causes of the Incident:

DNS Server Misconfiguration: The DNS server at 203.0.113.2 may not be configured to listen on UDP port 53. This could prevent it from responding to incoming DNS queries, thereby interrupting domain name resolution for the users.

Firewall or Network Policy Restrictions: There may be a firewall or network policy that blocks UDP traffic to port 53 on the DNS server. This could be due to incorrect firewall rules or restrictive network policies, preventing clients from accessing DNS serices.

Part 3 : Recommendations or Mitigations

· Verify DNS Server Configuration: Check that the DNS server at 203.0.113.2 is configured to accept requests on UDP port 53.

· Examine Firewall Settings: Review firewall and network policies to ensure that UDP traffic to port 53 is allowed.

· Use Alternate DNS Servers: If the issue cannot be immediately resolved, consider configuring clients to use an alternate DNS server for faster restoration of connectivity.

Part 4 : Conclusion

The incident likely stems from a misconfiguration in the DNS server or firewall restrictions that prevent DNS resolution. The inability to resolve the domain name means users cannot access the intended website.

Further investigation into the DNS server settings and network security policies is necessary to restore DNS functionality and website access.