Justin Goncalves

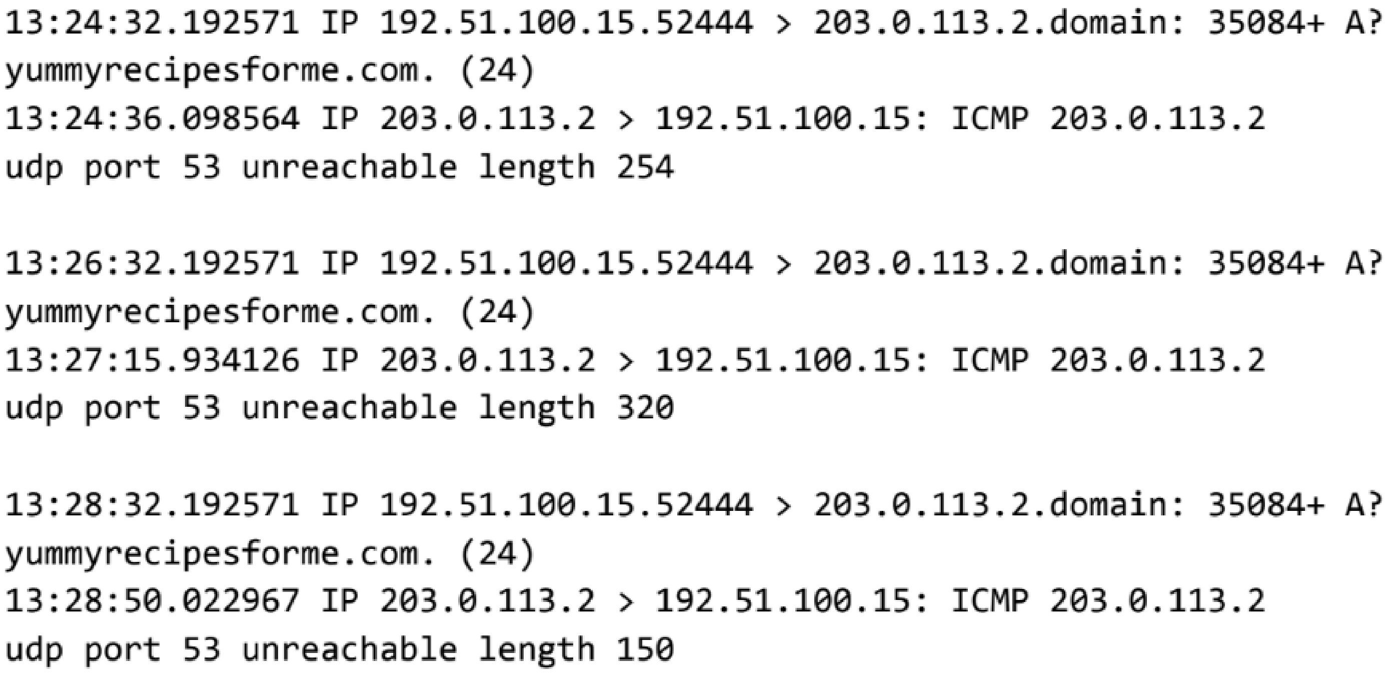
7/21/24

Cybersecurity Incident Report: TCPdump Network Traffic Analysis 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
```

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.

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
The UDP protocol analysis reveals that the browser sent a UDP packet to the DNS server at IP address 203.0.113.2 to retrieve the IP address for the domain www.yummyrecipesforme.com. This packet was intended for port 53, which is used by DNS services to handle such queries. The network analysis showed that the ICMP echo reply returned the error message "udp port 53 unreachable," indicating that the DNS server could not process the UDP packet sent to port 53. Since port 53 is used for DNS services, the most likely issue is that the DNS server is not properly configured to listen on this port, or the DNS service on this port is currently down or misconfigured.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident occurred at approximately 13:24:32, as indicated by the timestamps in the tcpdump log. The IT team became aware of the incident when several customers reported being unable to access the client company website www.yummyrecipesforme.com, encountering the error “destination port unreachable.” The IT department used the network analyzer tool, tcpdump, to capture and analyze the network traffic, confirming that the DNS query from the browser was sent via UDP to the DNS server at IP address 203.0.113.2 and directed to port 53. The DNS server responded with an ICMP error message indicating "udp port 53 unreachable." Subsequent DNS query attempts resulted in the same ICMP error, confirming the issue. The key findings indicate that the DNS server is either not running the DNS service on port 53, is misconfigured, or there are firewall rules or security settings blocking UDP traffic on port 53, causing the "destination port unreachable" error.