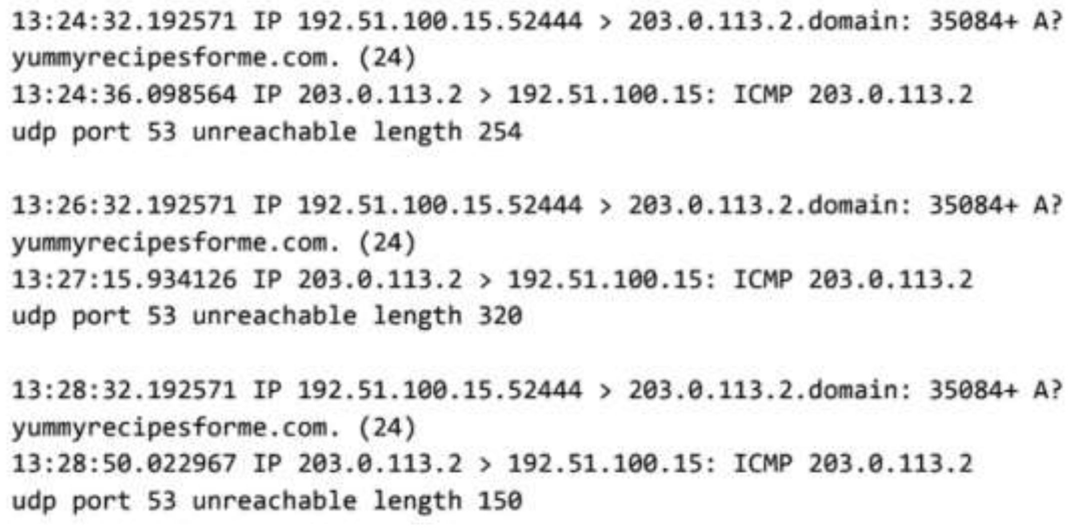
Manuela Kesten, February ’24.

Cybersecurity Incident Report:
Network Traffic Analysis

TASK:

Review the scenario below.

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.



```
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.

ANSWER:

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

The UDP protocol reveals that:
The initial outgoing request from the computer to the DNS server for resolving the domain name ‘yummyrecipesforme.com’ was sent using UDP. ICMP error messages indicate that the UDP packet was not deliverable to the DNS server, issue with destination port or service availability.

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

The port noted in the error message is used for:
Port 53 is used for DNS service. DNS is responsible for translating domain names to IP addresses and vice versa.

The most likely issue is:
There was no service listening on port 53 of the DNS server, leading to the UDP packet being undeliverable.

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

Time incident occurred:
It occurred at 13:24:32.192571. (1.24pm)

Explain how the IT team became aware of the incident:
IT team became aware through network monitoring tools or logs, which captured the failed UDP packet and subsequent ICMP error messages.

Explain the actions taken by the IT department to investigate the incident:
They likely started by reviewing network logs, such as tcpdump log provided, to understand the sequence of events leading to error. They may have also checked the configurations of the DNS server to ensure it was correctly set up to listen on port 53. They may have performed tests to verify connectivity to other services on the DNS server to rule out broader network issues.

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):
Key findings of the investigation would include confirmation that the DNS server was not listening on port 53, leading to undeliverable UDP packet. They may have also found that other services on the DNS server were functioning correctly, indicating that the issue was specific to port 53.

Note a likely cause of the incident:
A likely cause of the incident could be misconfiguration or a service failure on the DNS server, preventing it from listening on port 53. This could be due to software issues, firewall misconfigurations, or other administrative errors.