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
```

Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
The network protocol analyzer logs indicate that UDP port 53 on the DNS server located at 203.0.113.2 is unreachable when attempting to load the company website *www.yummyrecipesforme.com*. This is based on the ICMP echo reply, which returned the error message: *udp port 53 unreachable*. Therefore, the DNS server is down or unreachable. Port 53 is typically used for Domain Name Resolution. These logs may indicate a problem with the Domain Name Server configuration. It is highly likely that the DNS server is not responding. Alternatively, the server could be overwhelmed, potentially by an ongoing DDoS attack.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident occurred today at 13:23 UTC when several customers reported they were not able to access the company website *www.yummyrecipesforme.com*. They saw the error *destination port unreachable* after waiting for the page to load. In response, a PCAP was taken by the SIRT team with the tool *tcpdump* while attempting to load the aforementioned company website. The PCAP was analyzed to determine which network protocol and service were impacted by the incident. The network protocol analyzer logs indicated that UDP port 53 on the DNS server located at 203.0.113.2 is unreachable. We are continuing to investigate the root cause of the issue to determine how access to the DNS service can be restored. There may be a problem with the Domain Name Server configuration. Perhaps, port 53 is blocked on the firewall. Alternatively, the server could be overwhelmed, potentially by an ongoing DDoS attack.