Event scenario and associated event log

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

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
A part of DNS protocol The UDP protocol was used to conta contact the DNS server to retrieve the IP address for the domain name of yummyrecipesforme.com. 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.” Since port 53 is associated with DNS protocol traffic, we know this is an issue with the DNS server. Issues with performing the DNS protocol are further evident because because the plus sign after the query identification number 35084 indicates flags with the UDP message and the “A?” symbol indicates flags with performing DNS protocol operations. The most likely issue isThis may indicate a problem with the web server or the firewall configuration. It is possible that this is an indication of a malicious attack.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident occurred at 1:24 p.m. when Many customers reported that they were unable to access the client's company website www.yummyrecipesforme.com, and saw the error “Destination port could not be reached”.The network security team responded and began running tests with the network protocol analyzer tool tcpdump. The resulting logs revealed that port 53 which is used normally for DNS servers,is not reachable.We are continuing the investigation to reach the main root of the problem and work to solve it and return the operating mode to normal. Our next steps include checking the firewall to see if port 53 is blocked and communicating with the system administrator of the DNS server to have him scan the system for any attack. We believe that this is a type of attack. DNS server being disabled due to attack that made denial of service or misconfiguration , and its goal is to disrupt the website's functioning.