Cybersecurity Incident Report:
Network Traffic Analysis

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

The UDP protocol reveals that:

IP address for the website's domain name

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:

DNS service

The most likely issue is: UDP message requesting an IP address for the domain "www.yummyrecipesforme.com" did not go through to the DNS server because no service was listening on the receiving DNS port.

The network protocol analyzer logs indicate that port 53 is unreachable when attempting to access the **www.yummyrecipesforme.com** ***website. Port 53 is normally used for DNS service. This may indicate a DDoS attack that overwhelmed the system resulting in a DNS server shutdown. That means when users try to search for*** **www.yummyrecipesforme.com, a website** ***that used the DNS server was unreachable.***

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

Time incident occurred: 1:24 p.m., 32.192571 seconds

Explain how the IT team became aware of the incident: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.

Explain the actions taken by the IT department to investigate the incident: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.”

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):
error message indicating that the UDP packet was undeliverable to port 53 of the DNS server
Incident time is 1:24 p.m., 32.192571 seconds.
Destination IP address for the DNS server: 203.0.113.2.domain
For the ICMP error response, the source address is 203.0.113.2 and the destination is your computer's IP address 192.51.100.15.

Note a likely cause of the incident: UDP message requesting an IP address for the domain "www.yummyrecipesforme.com" did not go through to the DNS server because no service was listening on the receiving DNS port.

***The incident occurred in the afternoon around 1:24 p.m., 32.192571 seconds when 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. The cyber security team responded and began running tests with the network protocol analyzer tool tcpdump and attempted to load the page again. The resulting logs revealed that port 53, which is used for DNS service, is not reachable. The word "unreachable" in the message indicates the UDP message requesting an IP address for the domain "www.yummyrecipesforme.com" did not go through to the DNS server because no service was listening on the receiving DNS port*. So if DNS is unreachable then no IP address can be resolved resulting with the error “destination port unreachable”**

We are continuing to investigate the root cause of the issue to determine how we can restore the access to [*www.yummyrecipesforme.com*](http://www.yummyrecipesforme.com)*. Our next step is to check if the DNS server is having unusual traffic patterns or unusually high traffic. This will help us to determine if this is a DoS attack or not. Possible solution is a Traffic Filtering to eliminate known or malicious sources.*