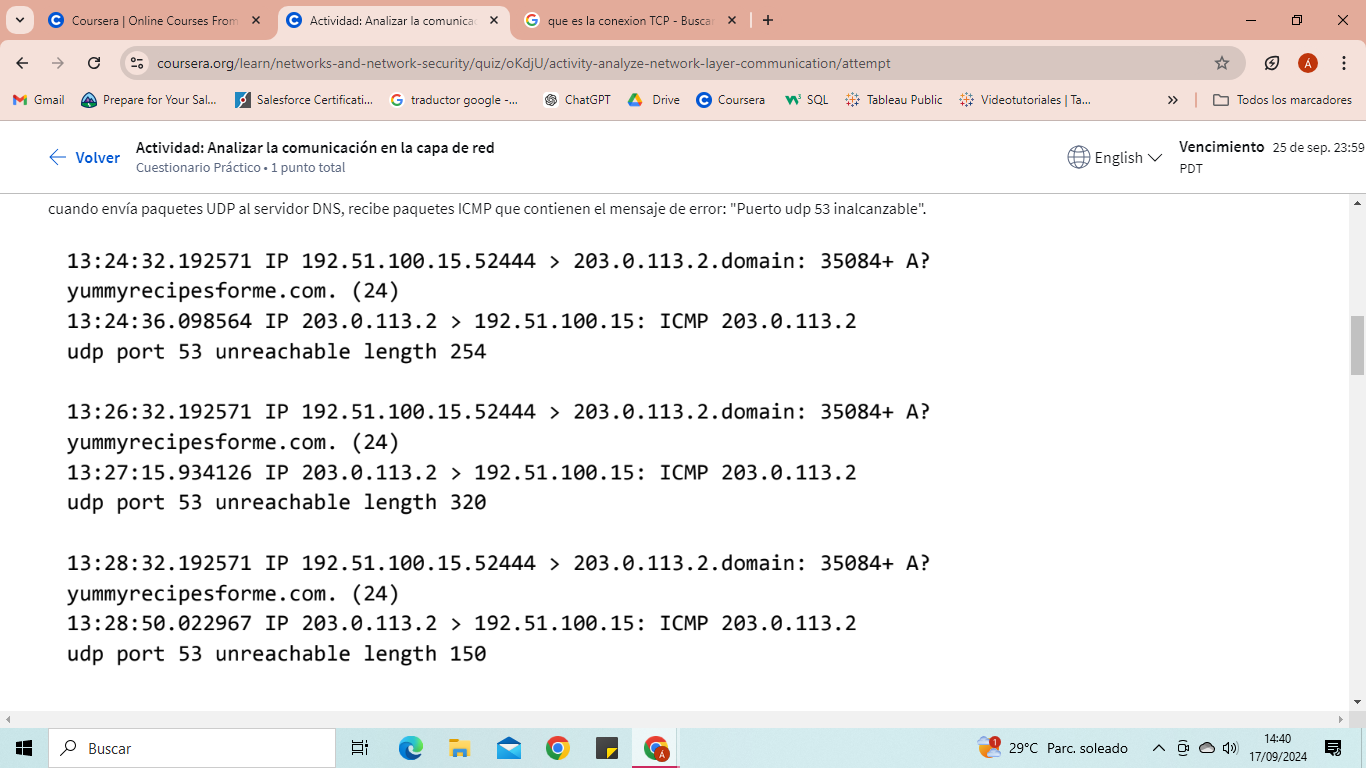
**Cybersecurity Incident Report:**

**Network Traffic Analysis**



**Analysis of the information received from tcpdump:**

The first two lines of the log file show the initial outgoing request from your computer to the DNS server requesting the IP address of yummyrecipesforme.com. This request is sent in a UDP packet.

The third and fourth lines of the log show the response to your UDP packet. In this case, the ICMP line 203.0.113.2 is the start of the error message indicating that the UDP packet could not be delivered to port 53 of the DNS server.

Before each request and response, you will find timestamps indicating when the incident occurred. In the log, this is the first sequence of numbers that appears: 13:24:32.192571. This means that the time is 13:24, 32.192571 seconds.

After the timestamps, you will find the source and destination IP addresses. In the first line, where the UDP packet travels from your browser to the DNS server, this information is shown as: 192.51.100.15 > 203.0.113.2.domain. The IP address to the left of the greater-than symbol (>) is the source address, which in this example is your computer's IP address. The IP address to the right of the greater-than symbol (>) is the destination IP address. In this case, it is the DNS server’s IP address: 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.

After the source and destination IP addresses, there may be additional details such as the protocol, source port number, and flags. In the first line of the error log, the query ID appears as: 35084. The plus sign after the query ID indicates that there are flags associated with the UDP message. The "A?" indicates a flag associated with a DNS request for an A record, where an A record maps a domain name to an IP address. The third line shows the protocol of the response message to the browser: "ICMP," followed by an ICMP error message.

The error message, "udp port 53 unreachable" is mentioned in the last line. Port 53 is a port for the DNS service. The word "unreachable" in the message indicates that the UDP message requesting an IP address for the domain "www.yummyrecipesforme.com" did not reach the DNS server because there was no service listening on the receiving DNS port.

The remaining lines of the log indicate that ICMP packets were sent two more times, but the same delivery error was received each time.

**Analysis of the data**

**Time incident occurred:** At 13:24:32.192571

**how the IT team became aware of the incident:** Several clients of the company reported that they could not access the client's website www.yummyrecipesforme.com and saw the error "destination port unreachable" after waiting for the page to load.

**the actions taken by the IT department to investigate the incident:** They tried to visit the website themselves and also received the "destination port unreachable" error. To investigate the issue, they loaded their network analysis tool, tcpdump, and tried to reload the website. To load the website, their browser sends a query to a DNS server via UDP to retrieve the IP address of the website’s domain name; this is part of the DNS protocol. Then, the browser uses this IP address as the destination IP to send an HTTPS request to the web server to display the website. The analyzer shows that when sending UDP packets to the DNS server, it receives ICMP packets containing the error message: "UDP port 53 unreachable."

**Note a likely cause of the incident**

* Verify the DNS Service on the Server: The error message "UDP port 53 unreachable" indicates that the DNS server is not available on port 53, which is the standard port for DNS services. Ensure that the DNS service is running on the server you are trying to connect to. This may involve checking that the DNS server is powered on and that DNS software (such as BIND, Unbound, or the DNS service on a Windows server) is running correctly.
* Check Network Configuration: Make sure there are no network issues preventing the connection. This includes checking that there are no blocks in the firewall or security rules that are blocking UDP traffic on port 53. If you have control over the DNS server, verify firewall settings on both the server and any intermediate devices (such as routers or firewalls) to ensure that they allow traffic on port 53.
* Review Client Configuration: Verify that your client (browser or application) is correctly configured to use the DNS server. Ensure that the DNS settings on your device or in your network are pointing to the correct DNS server.
* Restart Network Equipment: Sometimes, restarting the router, DNS server, or client device can resolve temporary network issues.