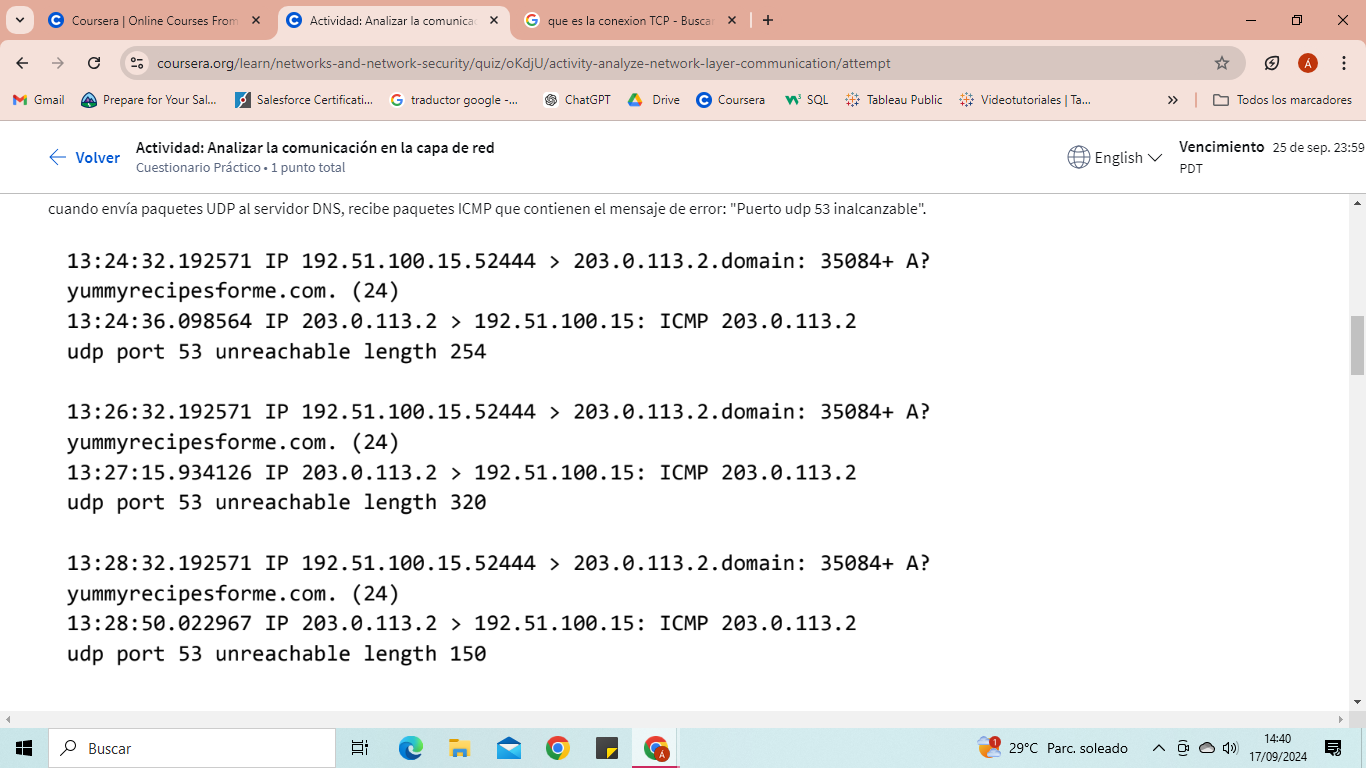
**Informe de incidentes de ciberseguridad:**

**Análisis de tráfico de red**



**Análisis de la información recibida de tcpdump:**

Las dos primeras líneas del archivo de registro muestran la solicitud saliente inicial desde su computadora al servidor DNS solicitando la dirección IP de yummyrecipesforme.com. Esta solicitud se envía en un paquete UDP.

La tercera y cuarta líneas del registro muestran la respuesta a su paquete UDP. En este caso, la línea ICMP 203.0.113.2 es el comienzo del mensaje de error que indica que el paquete UDP no se pudo entregar al puerto 53 del servidor DNS.

Antes de cada solicitud y respuesta, encontrará marcas de tiempo que indican cuándo ocurrió el incidente. En el registro, esta es la primera secuencia de números que aparece: 13:24:32.192571. Esto significa que el tiempo es 13:24, 32,192571 segundos.

Después de las marcas de tiempo, encontrará las direcciones IP de origen y destino. En la primera línea, donde viaja el paquete UDP desde su navegador al servidor DNS, esta información se muestra como: 192.51.100.15 > 203.0.113.2.domain. La dirección IP a la izquierda del símbolo mayor que (>) es la dirección de origen, que en este ejemplo es la dirección IP de su computadora. La dirección IP a la derecha del símbolo mayor que (>) es la dirección IP de destino. En este caso, es la dirección IP del servidor DNS: 203.0.113.2.dominio. Para la respuesta de error ICMP, la dirección de origen es 203.0.113.2 y el destino es la dirección IP de su computadora 192.51.100.15.

Después de las direcciones IP de origen y destino, puede haber detalles adicionales como el protocolo, el número de puerto de origen y las banderas. En la primera línea del registro de errores, el ID de la consulta aparece como: 35084. El signo más después del ID de la consulta indica que hay indicadores asociados con el mensaje UDP. La "A?" indica un indicador asociado con una solicitud DNS para un registro A, donde un registro A asigna un nombre de dominio a una dirección IP. La tercera línea muestra el protocolo del mensaje de respuesta al navegador: "ICMP", seguido de un mensaje de error ICMP.

El mensaje de error "puerto udp 53 inalcanzable" se menciona en la última línea. El puerto 53 es un puerto para el servicio DNS. La palabra "inalcanzable" en el mensaje indica que el mensaje UDP que solicita una dirección IP para el dominio "www.yummyrecipesforme.com" no llegó al servidor DNS porque no había ningún servicio escuchando en el puerto DNS receptor.

Las líneas restantes del registro indican que los paquetes ICMP se enviaron dos veces más, pero cada vez se recibió el mismo error de entrega.

**Análisis de los datos**

**Hora en que ocurrió el incidente:** A las 13:24:32.192571

**Cómo el equipo de TI se enteró del incidente:** Varios clientes de la empresa informaron que no pudieron acceder al sitio web del cliente www.yummyrecipesforme.com y vieron el error "puerto de destino inalcanzable" después de esperar a que se cargara la página.

**Las acciones tomadas por el departamento de TI para investigar el incidente:** Intentaron visitar el sitio web ellos mismos y también recibieron el error "puerto de destino inalcanzable". Para investigar el problema, cargaron su herramienta de análisis de red, tcpdump, e intentaron recargar el sitio web. Para cargar el sitio web, su navegador envía una consulta a un servidor DNS a través de UDP para recuperar la dirección IP del nombre de dominio del sitio web; esto es parte del protocolo DNS. Luego, el navegador utiliza esta dirección IP como IP de destino para enviar una solicitud HTTPS al servidor web para mostrar el sitio web. El analizador muestra que al enviar paquetes UDP al servidor DNS, recibe paquetes ICMP que contienen el mensaje de error: "Puerto UDP 53 inalcanzable".

**Tenga en cuenta una causa probable del incidente**

* Verifique el servicio DNS en el servidor: el mensaje de error "Puerto UDP 53 inalcanzable" indica que el servidor DNS no está disponible en el puerto 53, que es el puerto estándar para los servicios DNS. Asegúrese de que el servicio DNS se esté ejecutando en el servidor al que intenta conectarse. Esto puede implicar verificar que el servidor DNS esté encendido y que el software DNS (como BIND, Unbound o el servicio DNS en un servidor Windows) se esté ejecutando correctamente.
* Verifique la configuración de red: asegúrese de que no haya problemas de red que impidan la conexión. Esto incluye verificar que no haya bloqueos en el firewall o reglas de seguridad que bloqueen el tráfico UDP en el puerto 53. Si tiene control sobre el servidor DNS, verifique la configuración del firewall tanto en el servidor como en cualquier dispositivo intermedio (como enrutadores o firewalls). para garantizar que permitan el tráfico en el puerto 53.
* Revisar la configuración del cliente: Verifique que su cliente (navegador o aplicación) esté configurado correctamente para usar el servidor DNS. Asegúrese de que la configuración de DNS en su dispositivo o en su red apunte al servidor DNS correcto.
* Reinicie el equipo de red: a veces, reiniciar el enrutador, el servidor DNS o el dispositivo cliente puede resolver problemas temporales de la red.