ANÁLISIS DEL TRÁFICO DE RED

Parte 1: Proporciona un resumen del problema encontrado en el registro de tráfico DNS e ICMP	**Explicación**
A. El uso del protocolo UDP indica que el servidor DNS está caído o inaccesible. B. Los resultados del análisis de red muestran que la respuesta de eco ICMP devolvió el mensaje de error "udp port 53 unreachable" (puerto UDP 53 inaccesible). C. El puerto 53 se utiliza comúnmente para el tráfico del protocolo DNS, lo que sugiere que el servidor DNS probablemente no esté respondiendo.	A. En el escenario se muestra el protocolo utilizado para gestionar las comunicaciones y el puerto al que se dirigieron. En el registro de errores, esto se presenta como "udp port 53 unreachable" (puerto UDP 53 inaccesible). Esto indica que se utilizó el protocolo UDP para solicitar una resolución de nombre de dominio a través del puerto 53 del servidor DNS. B. Se realizó un análisis de red con tcpdump, el cual registró paquetes ICMP desde la computadora de origen hasta la dirección IP y el puerto del sitio web (203.0.113.2.domain). También se registraron respuestas ICMP del sitio web hacia la computadora de origen. Al revisar los registros de errores DNS e ICMP, se observa que las respuestas ICMP incluyen un tipo de mensaje de error, que tcpdump muestra como "udp port 53 unreachable" (puerto UDP 53 inaccesible). C. Los problemas observados en los registros pueden interpretarse como una inaccesibilidad al puerto 53, que es comúnmente utilizado para comunicaciones del protocolo DNS. Esto sugiere que el servidor DNS no está respondiendo o es inaccesible. Una posible causa podría ser un ataque de denegación de servicio (DoS) dirigido contra el servidor DNS, impidiendo su funcionamiento normal.

Parte 2: Explica tu análisis de los datos y proporciona una solución para implementar	**Explicación**
D. El incidente tuvo lugar hoy a la 1:23 p.m.	D. Esta información fue obtenida a partir de las marcas de fecha y hora en el archivo de registro. En el registro, la primera secuencia de números que aparece es 13:24:32.192571, lo que indica que el evento ocurrió a las 13:24 con 32.192571 segundos, utilizando un formato de 24 horas. El escenario especifica que este evento ocurrió el mismo día.
E. Las y los clientes se comunicaron con la organización para informar al equipo de TI que recibían el mensaje "puerto de destino inaccesible" al intentar acceder al sitio web.	E. El escenario describe que varios clientes se comunicaron con la empresa para informar que no podían acceder al sitio web de la compañía, y que recibieron el error "puerto de destino inaccesible" después de intentar cargar la página.
F. Los profesionales de seguridad de la red de la organización están investigando el problema para restaurar el acceso al sitio web para las y los clientes.	F. Según el escenario, este incidente está siendo gestionado por ingenieros de seguridad, luego de que tanto el analista como otros colegas informaran del problema al supervisor directo.
G. Durante la investigación del problema, se realizaron pruebas de rastreo de paquetes utilizando tcpdump. En el archivo de registro resultante, se descubrió que el puerto DNS 53 era inaccesible.	G. El escenario relata que al visitar el sitio web, el analista también recibe el error "puerto de destino inaccesible". Luego, utiliza la herramienta de análisis de red tcpdump y recarga la página web. En esta ocasión, recibe una gran cantidad de paquetes en el analizador de red. Al enviar paquetes UDP, recibe una respuesta ICMP con el mensaje de error "udp port 53 unreachable" (puerto UDP 53 inaccesible).

H. El próximo paso es determinar si el servidor DNS está inactivo o si el firewall está bloqueando el tráfico al puerto 53.	H. En caso de que el servidor DNS esté funcionando correctamente, el equipo debe revisar la configuración del firewall para verificar si alguien ha cambiado la configuración, bloqueando el tráfico en el puerto 53. Los firewalls permiten bloquear el tráfico en puertos específicos, y el bloqueo de puertos puede utilizarse para detener o prevenir un ataque.
I. El servidor DNS podría estar fuera de servicio debido a un ataque de denegación de servicio exitoso o a una configuración errónea.	I. El objetivo de un ataque de denegación de servicio (DoS) es enviar una gran cantidad de información a un dispositivo de red, como un servidor DNS, para bloquearlo o impedir que responda al tráfico legítimo. Es posible que un atacante haya deshabilitado el servidor DNS con un ataque DoS, o que alguien del equipo haya realizado un cambio en la configuración del firewall que resultó en el bloqueo del puerto 53.