Explicación del ejemplo
Informe sobre incidentes de ciberseguridad: Análisis del tráfico de red

Parte 1: Proporciona un resumen del problema encontrado en el registro de tráfico DNS e ICMP	Explicación
A. El protocolo UDP revela que el servidor DNS está caído o inaccesible. B. Como evidencian los resultados del análisis de la red, la respuesta de eco ICMP devolvió el mensaje de error "udp port 53 unreachable" (puerto udp 53 inaccesible). C. El puerto 53 se usa habitualmente para el tráfico del protocolo DNS. Es muy probable que el servidor DNS no responda.	A. **Ofrece un breve resumen del análisis de los registros DNS e ICMP.** Siguiendo las instrucciones, deberías haber identificado “qué protocolo y servicio de red se vieron afectados por este incidente”. En el escenario se indica: “[El archivo de registro] muestra qué protocolo se utilizó para gestionar las comunicaciones y a qué puerto se entregó. En el registro de errores, esto se muestra como "udp port 53 unreachable" (puerto udp 53 inaccesible). Esto significa que el protocolo UDP se usó para solicitar una resolución de nombre de dominio utilizando la dirección para el servidor DNS a través del puerto 53”. B. **Proporciona algunos detalles sobre lo que se indicó en los registros:** La sección Escenario indica que realizaste un análisis de red utilizando tcpdump, que registró paquetes ICMP desde tu computadora de origen a la dirección IP y el puerto del sitio web (203.0.113.2.domain). También registró las respuestas ICMP desde el sitio web hacia tu computadora. Si revisas el registro de errores DNS e ICMP, las respuestas ICMP incluyen un tipo de mensaje de error, que tcpdump representa como "udp port 53 unreachable" (puerto udp 53 inaccesible). C. **Interpreta los problemas encontrados en los registros.** La sección Escenario (o una búsqueda rápida en Internet de “puerto 53”) mostrará que este número de puerto se usa habitualmente para comunicaciones del protocolo DNS. Dado que el puerto 53 es inaccesible y que ese puerto se usa comúnmente para las comunicaciones del servidor

	DNS, puedes concluir que el servidor DNS es inaccesible o “no responde”. Esto podría ser causado por un ataque DoS contra el servidor DNS, por ejemplo.

Parte 2: Explica tu análisis de los datos y proporciona una solución para implementar	Explicación
D. El incidente ocurrió hoy a la 1:23 p. m. E. Las/los clientes llamaron a la organización para notificar al equipo de TI que recibían el mensaje “puerto de destino inaccesible” cuando intentaban visitar el sitio web. F. Las/los profesionales de seguridad de la red de la organización están investigando el problema para que las/los clientes puedan acceder al sitio web nuevamente.	D. **Indica cuándo se notificó el problema por primera vez:** Esta información se obtuvo de las marcas de fecha y hora del archivo de registro. En el registro, esta es la primera secuencia de números que se muestra: 13:24:32.192571. Esto muestra la hora 1:24 p. m., 32.192571 segundos, con la hora en formato de 24 horas. El Escenario indica que este evento ocurrió hoy. E. **Proporciona el escenario, los eventos y los síntomas identificados cuando se informó por primera vez del evento:** El Escenario establece que “Un puñado de clientes se comunicaron con tu empresa para reportar que no podían acceder al sitio web de la compañía y vieron el error “puerto de destino inaccesible” después de esperar que la página se cargara”. F. **Explica el estado actual del problema:** El Escenario establece que: “Este incidente, mientras tanto, está siendo manejado por ingenieros de seguridad después de que tanto tú como otros

G. En nuestra investigación del problema, realizamos pruebas de rastreo de paquetes utilizando tcpdump. En el archivo de registro resultante, encontramos que el puerto DNS 53 era inaccesible.	analistas hayan informado del problema a tu supervisor directo". G. **Describe la información descubierta en la investigación del problema hasta este momento:** Proporciona un resumen conciso de lo que hiciste para investigar el problema. El Escenario dice: "Visitas el sitio web y también recibes el error 'puerto de destino inaccesible'". A continuación, cargas tu herramienta de análisis de red, tcpdump, y vuelves a cargar la página web. Esta vez, recibes una gran cantidad de paquetes en tu analizador de red. En el analizador, envías paquetes UDP y recibes una respuesta ICMP para regresar al host. Los resultados contienen un mensaje de error: "udp port 53 unreachable" (puerto udp 53 inaccesible).
H. El siguiente paso es identificar si el servidor DNS está caído o si el tráfico al puerto 53 está bloqueado por el cortafuegos.	H. **Enumera los siguientes pasos para solucionar el problema:** El siguiente paso para solucionar el problema es determinar si el servidor DNS no funciona correctamente. Si el servidor DNS está bien, el equipo debe verificar la configuración del cortafuegos (firewall) para ver si alguien cambió la configuración para bloquear el tráfico de red en el puerto 53. Los firewalls ofrecen la capacidad de bloquear el tráfico de red en puertos específicos. El bloqueo de puertos se puede utilizar para detener o prevenir un ataque.
I. El servidor DNS podría estar caído debido a un ataque de denegación de servicio exitoso o una configuración incorrecta.	I. **Proporciona la presunta causa raíz del problema:** Anteriormente, aprendiste acerca de varios tipos de ataques de denegación de servicio (DoS). El objetivo de un ataque DoS es enviar una gran cantidad de información a un dispositivo de red, como un servidor DNS, para bloquearlo o hacer que sea incapaz de responder al tráfico de red legítimo. Es posible que un/a atacante haya desactivado el servidor DNS con un ataque DoS. Otra posibilidad es que alguien de tu equipo haya realizado un cambio de configuración en el firewall que resultó en el bloqueo del puerto 53.