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.
El protocolo UDP revela que el servidor DNS está caído o inaccesible. Como se desprende de los resultados del análisis de red, la respuesta de eco ICMP devolvió el mensaje de error "udp port 53 unreachable" (puerto udp 53 inaccesible). El puerto 53 se usa habitualmente para el tráfico del protocolo DNS. Es muy probable que el servidor DNS no esté respondiendo.

Parte 2: Explica tu análisis de los datos y proporciona una solución para implementar.
El incidente ocurrió hoy a la 1:23 p.m. 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. 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. 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. El siguiente paso es identificar si el servidor DNS está caído o si el tráfico al puerto 53 está bloqueado por el cortafuegos. El servidor DNS podría estar caído debido a un ataque de denegación de servicio exitoso o una configuración incorrecta.