# Informe de incidentes de ciberseguridad: análisis del tráfico de la red

| Parte 1: Proporcione un resumen del problema encontrado en el DNS y el ICMP  registro de tráfico | |
| --- | --- |
| El protocolo UDP revela que el servidor DNS está inactivo o no se puede acceder a él. Como se desprende de los resultados del análisis de red, la respuesta de eco ICMP devolvió el mensaje de error “puerto udp 53 inalcanzable”. El puerto 53 se utiliza habitualmente para el tráfico del protocolo DNS. Es muy probable que el servidor DNS no esté respondiendo. | |
|

| Parte 2: Explique su análisis de los datos y proporcione una solución para implementar. |
| --- |
| El incidente ocurrió hoy a las 13:23. Los clientes llamaron a la organización para notificar al equipo de TI que recibieron el mensaje “puerto de destino inalcanzable” cuando intentaron visitar el sitio web. Los profesionales de seguridad de red de la organización están investigando el problema para que los clientes puedan acceder nuevamente al sitio web. En nuestra investigación sobre el problema, realizamos pruebas de detección de paquetes con tcpdump. En el archivo de registro resultante, descubrimos que el puerto DNS 53 era inalcanzable. El siguiente paso es identificar si el servidor DNS está inactivo o si el firewall bloquea el tráfico al puerto 53. El servidor DNS podría estar inactivo debido a un ataque de denegación de servicio exitoso o una configuración incorrecta. |