INFORME SOBRE INCIDENTES DE CIBERSEGURIDAD: ANÁLISIS DEL TRÁFICO DE RED

Parte 1: Resumen del problema encontrado en el registro de tráfico DNS e ICMP.
El uso del protocolo UDP sugiere que el servidor DNS está caído o inaccesible. Según los resultados del análisis de red, la respuesta de eco ICMP incluyó el mensaje de error "udp port 53 unreachable" (puerto UDP 53 inaccesible). Dado que el puerto 53 se utiliza comúnmente para el tráfico del protocolo DNS, es probable que el servidor DNS no esté respondiendo.

Parte 2: Análisis de los datos y posible solución para implementar.
El incidente tuvo lugar hoy a la 1:23 p.m. 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. Los profesionales de seguridad de la red de la organización están investigando el problema para restaurar el acceso al sitio web para los clientes. Durante la investigación, se realizaron pruebas de rastreo de paquetes utilizando tcpdump, y en el archivo de registro resultante se encontró que el puerto DNS 53 era inaccesible. El siguiente paso es determinar si el servidor DNS está caído o si el firewall está bloqueando el tráfico al puerto 53. Es posible que el servidor DNS esté inactivo debido a un ataque de denegación de servicio exitoso o a una configuración incorrecta.