Un servidor Linux crítico para la infraestructura de una empresa ha mostrado signos de actividad sospechosa. Durante una auditoría rutinaria, se ha identificado la presencia de un binario desconocido ubicado en un directorio no estándar. La naturaleza y el origen de este archivo son inciertos, pero su comportamiento sugiere una posible manipulación del sistema.

El equipo de seguridad ha solicitado un análisis para comprender el alcance de su impacto. Esto incluye identificar cualquier cambio realizado en la configuración del sistema, los posibles vectores de ataque utilizados, y evaluar si este binario representa una amenaza activa.

Para completar esta tarea, deberás inspeccionar el servidor en busca de evidencias relacionadas con este binario, evaluar su comportamiento, y documentar tus hallazgos. Es fundamental que determines:

1. La función principal del binario.
2. Si ha modificado archivos del sistema o configuraciones críticas.
3. Cualquier rastro que indique cómo llegó al servidor.
4. Su posible relación con eventos anómalos registrados en el sistema.

Tu análisis debe ser sistemático y centrarse en obtener conclusiones claras sobre el impacto del binario en el sistema. Evita confiar en herramientas avanzadas; utiliza únicamente las capacidades básicas disponibles en un entorno estándar de Linux para simular las restricciones de un equipo de respuesta inicial.

Login: root / toor