Profundiza más

Recurso de Profundización

Estudio de Caso 1: Detección de IP sospechosa en registros de acceso
En el estudio de caso presentado se muestra un ejemplo claro de cómo los algoritmos de búsqueda permiten identificar y localizar actividad sospechosa dentro de grandes volúmenes de información. Además, el uso de algoritmos de búsqueda eficientes permite optimizar los tiempos de análisis y mejorar la capacidad de respuesta ante incidentes. Esto resulta especialmente importante en entornos de ciberseguridad, donde es necesario procesar grandes cantidades de datos en tiempo real.

Contexto
Una empresa monitorea accesos a su servidor. El analista de seguridad necesita verificar si una dirección IP reportada como sospechosa aparece en los registros del día.

Datos disponibles
Registro de 5,000 direcciones IP almacenadas en un archivo de logs.

Problema
Buscar la IP: **185.43.21.90**

Solución aplicada
Se utiliza **búsqueda lineal**, porque:

- Los logs no están ordenados.
- Se agregan registros constantemente.

Funcionamiento
El sistema revisa cada registro hasta encontrar la IP o terminar la lista.

Resultado

- Se encuentra la IP en la posición 4,200.
- Se detectan 15 intentos de acceso fallidos.

Análisis

- Complejidad: O(n)
- Ventaja: No requiere ordenar datos
- Desventaja: Puede ser lenta en grandes volúmenes

Aprendizaje clave
La búsqueda lineal es útil cuando los datos cambian constantemente o no están organizados.