Tecnológico de Monterrey

Programación de estructuras de datos y algoritmos fundamentales (Gpo 602)

Act 1.3 - Actividad Integral de Conceptos Básicos y Algoritmos Fundamentales (Evidencia Competencia)

investigación y reflexión en forma individual de la importancia y eficiencia del uso de los diferentes algoritmos de ordenamiento y búsqueda en una situación problema de esta naturaleza

21/09/2025

Profesor

Daniel Perez R

Alumno

José Luis Gutiérrez Quintero A01739337

Reflexión sobre la importancia y eficiencia de los algoritmos de ordenamiento y búsqueda en la detección de botnets.

Yo considero que las botnets representan una de las amenazas más persistentes y dañinas. Según TechTarget (s.f.), una botnet es una red de dispositivos comprometidos que pueden ser utilizados de forma remota para realizar ataques coordinados, como el envío masivo de spam, fraudes o la interrupción de servicios. El FBI ha señalado que este tipo de ataques ha crecido de manera preocupante, llegando a provocar pérdidas significativas en diversos sectores. Como lo describe Condliffe (2017) en MIT Technology Review, aunque se han desmantelado redes de bots, la magnitud del problema requiere métodos cada vez más eficientes para analizar grandes volúmenes de información y detectar accesos maliciosos a tiempo.

la informática nos brinda las herramientas para trabajar con datos masivos de registros o *logs* de acceso. El reto principal no es solo almacenar, sino poder ordenar y buscar en estos datos de manera rápida y confiable. De acuerdo con Knuth (1998) y Cormen et al. (2022), los algoritmos de ordenamiento constituyen la base para optimizar la búsqueda. Ordenar primero permite que operaciones posteriores, como encontrar un rango de fechas o detectar patrones en direcciones IP, se realicen con mayor eficiencia. Por ejemplo, QuickSort, utilizado en la práctica desarrollada, ofrece una complejidad promedio de O (n log n), lo que lo hace muy adecuado para trabajar con bitácoras medianas o grandes en memoria. Otros algoritmos como Bubble Sort o Insertion Sort, aunque más sencillos, se vuelven ineficientes en escenarios de datos extensos, pues su complejidad $O(n^2)$ ralentiza el análisis. En cambio, para volúmenes masivos de datos que no caben en memoria, autores como Sedgewick y Wayne (2011) recomiendan algoritmos externos como Merge Sort.

El uso de estructuras de datos también influye en la eficiencia. En este proyecto, un vector resultó suficiente para almacenar y procesar los registros, pero Weiss (2014) plantea que estructuras como tablas hash o árboles balanceados son más adecuadas cuando se requiere acceso más directo, agrupaciones por IP o consultas frecuentes. Además, la búsqueda implementada en la práctica utilizó un esquema de rango con claves inclusivas (00:00:00 a 23:59:59), lo cual asegura que no se pierdan registros y permite un “corte temprano” una vez superado el límite superior, optimizando el recorrido.

La relación con la detección de botnets se observa en que, al ordenar y filtrar de forma eficiente los accesos, es posible distinguir entre tráfico legítimo y accesos maliciosos. Un acceso puede

considerarse sospechoso si proviene de un mismo rango de IPs con demasiadas solicitudes en un periodo corto, si utiliza puertos inusuales o si aparece asociado a patrones de error repetitivos. Agrupar los registros por estas características facilita la identificación de comportamientos anómalos. Así, los algoritmos de ordenamiento y búsqueda no son solo una cuestión académica, sino una herramienta clave en la lucha contra ataques coordinados.

Sintetizando esta reflexión: la eficiencia en ciberseguridad depende en gran parte de la capacidad de analizar datos rápidamente. Ordenar las bitácoras permite acelerar la búsqueda y obtener resultados más confiables. QuickSort se muestra práctico en la práctica académica, mientras que otros algoritmos más robustos podrían emplearse en escenarios de mayor escala. La combinación de buenas estructuras de datos y algoritmos adecuados es esencial para transformar registros aparentemente caóticos en información clara que permita prevenir y combatir el fenómeno de las botnets.

Referencias

- Condliffe, J. (2017, April 10). *The FBI shut down a huge botnet, but there are plenty more left*. MIT Technology Review. https://www.technologyreview.com/s/604138/the-fbi-shut-down-a-huge-botnet-but-there-are-plenty-more-left/
- TechTarget. (s.f.). *Botnet*. SearchSecurity. https://www.techtarget.com/searchsecurity/definition/botnet
- Cormen, T. H., Leiserson, C. E., Rivest, R. L., & Stein, C. (2022). *Introduction to Algorithms* (4th ed.). MIT Press.
- Knuth, D. E. (1998). *The Art of Computer Programming, Volume 3: Sorting and Searching* (2nd ed.). Addison-Wesley.
- Sedgewick, R., & Wayne, K. (2011). *Algorithms* (4th ed.). Addison-Wesley.
- Weiss, M. A. (2014). *Data Structures and Algorithm Analysis in C++* (4th ed.). Pearson