



Tecnológico
de Monterrey

REFLEXIÓN - ACT 3 INTEGRAL

DANTE HERNÁNDEZ RAMÍREZ - A01668070

Programación de estructuras de datos y algoritmos fundamentales
(Gpo 573)

29 de Enero del 2026

Reflexión

La ciberseguridad tiene la función de proteger datos, dispositivos y redes de delincuentes y demás tipos de daños posibles al sistema. En este ámbito, la ciberseguridad es un ámbito sumamente importante, ya que las medidas inadecuadas podrían comprometer la información de los usuarios o empresas, llegando a afectar de forma grave a los mismos.

En concreto, el sistema de la actividad trata de identificar las direcciones IPv4 que tuvieron un mayor número de accesos. La actividad tiene como base general el análisis de los registros más visitados, en el siguiente orden:

- Lectura de los registros.
- Ordenamiento de los mismos registros.
- Aplicación de una estructura de datos para la obtención de la información objetiva.

ESTRUCTURAS DE DATOS JERÁRQUICAS

Para el análisis de grandes volúmenes de datos (como el de la actividad propuesta). Para el diseño de la estructura se seleccionó el Binary Heap sobre un BST, ya que aunque ambas estructuras se basan en árboles, el BST toma como base las búsquedas arbitrarias. Sin embargo, para esta actividad, se requiere obtener las mismas IP con mayor frecuencia.

Para este propósito, el Binary Heap seleccionado permite acceder al elemento que posee mayor prioridad en un tiempo constante. Agregado a esto, con la ayuda de la implementación de un vector se registran los datos en la memoria de manera continua.

ANÁLISIS DE COMPLEJIDAD:

La solución implementada con la estructura de datos jerárquica, la solución implementada se podría catalogar como eficiente:

- Lectura del archivo: $O(n)$
- Ordenamiento con Heap: $O(n \log(n))$
- Conteo de accesos de los registros de IP: $O(n)$
- Obtención del Top 10 de IP: $O(10 \log(n))$

Se podría generalizar la complejidad total del sistema como $O(n \log(n))$, lo cuál podría clasificar como un buen desempeño en registros de mediano o gran tamaño.

UTILIDAD DE DETECCIÓN DE AMENAZAS

Este algoritmo se usa como referencia para el análisis de seguridad de los registros de las IP. Algunos de los indicadores son precisamente la frecuencia de accesos de una misma red. El uso de Heapsort y Binary Heap cumple más allá de los requerimientos necesarios o mínimos, sino que además garantiza la eficiencia de desempeño coherente para el análisis de los registros.

Agregado a esto, las estructuras jerárquicas dan la posibilidad de actuar con prevención para un posible ataque a las IP con mayores registros de accesos.

CONCLUSIÓN

Con esta actividad se requirió la selección a conciencia de una estructura de datos adecuada para el funcionamiento del algoritmo. Un correcto análisis de complejidad, más allá de un ámbito teórico, en un entorno más cercano a la realidad, marca la diferencia respecto a la resolución de los problemas. El uso correcto entre una lista ordenada o un Binary Heap marca la agilidad y la eficiencia al momento de detectar intrusos.

REFERENCIAS

Cormen, T. H., Leiserson, C. E., Rivest, R. L., & Stein, C. (2022). Introducción a los algoritmos (4th ed.). MIT Press.

<https://mitpress.mit.edu/9780262046305/introduction-to-algorithms/>

Heap sort. GeeksforGeeks. <https://www.geeksforgeeks.org/heap-sort/>

Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press.
<https://global.oup.com/academic/product/cybersecurity-and-cyberwar-9780190654102>