Tecnológico de Monterrey

Reflexión 4.3

Alfonso José Morales Mallozzi
A00841550

La actividad 4.3 me obligó a desarrollar una aplicación la cual manejara una bitacora de ips. la cual estaban registradas de una manera desordenada la cual requeria que se solucionara este mismo problema usando estructuras de datos adecuadas y algoritmos precisos y eficaces para el problema presentado, pues estas misma organización de las ips nos permitiria observar conexiones y patrones de comunicación, identificando nodos críticos y estimar comportamientos los cuales sean maliciosos dentro de la situación.

Importancia del uso de grafos en esta problemática

El uso de grafos resulta fundamental en problemas de análisis de tráfico de red y ciberseguridad, ya que permite representar de manera natural las relaciones entre entidades (IPs) y sus interacciones. Modelar la bitácora como una lista de adyacencia facilita:

- Identificar nodos con alta actividad (alto grado de salida), los cuales pueden indicar control, propagación o comportamiento anómalo.
- Analizar la conectividad y el alcance de un nodo dentro de la red.
- Aplicar algoritmos clásicos de grafos para extraer información relevante, como caminos más cortos o nodos más influyentes.

Eficiencia y complejidad computacional

Se usó una lista de adyacencia la cual resulta ser eficiente en los tipos de grafos presentes que se encuentran en los tráficos de red, pues la lectura del archivo y la construcción del grafo presente en este mismo tiene una complejidad aproximada de O(n), pues n es el número de registros que estará en la bitácora

El cálculo del grado de salida de cada IP se realiza recorriendo la lista de adyacencia, lo cual también es **O(V + E)**, siendo *V* el número de nodos e *E* el número de aristas. Se logró usar una estructura heap la cual me permitió detectar y encontrar las 7 ips más notables que se presenten maliciosas, lo que permitió mantener un orden eficiente con una complejidad de **O(n log n)** en el peor de los casos.

La tarea de encontrar los caminos más cortos desde el boot master fue realizada mediante un algoritmo de búsqueda de caminos mínimos el cual sea adecuado para el modelo del grafo presente dentro de la estructura con la que estamos trabajando, pues esta misma me permite calcular las distancias de una forma sistemática y sobre todo eficiente. Este análisis hizo posible identificar la ip que requiere el mayor esfuerzo de ataque, dandonos como resultado la mayor distancia respecto al nodo origen con el que se está trabajando.

Reflexión sobre la toma de decisiones

Se tuvo que hacer un intento y error varias veces debido a la selección de las estructuras y algoritmos, pues estos mismos deben ser adecuados para cuando se trabaja con este tipo de problemas. Elegir listas de adyacencia y heaps respondió a este mismo proceso para implementarlo de una manera correcta nuestra solución hacia el problema presente.

Asimismo, la identificación del *boot master* no se basa en una certeza absoluta, sino en inferencias obtenidas a partir del grado de salida y la conectividad del grafo, lo cual refleja una situación realista en el análisis de redes y seguridad.

Conclusión

La actividad me dejo varios conocimientos teóricos en el area de redes, especialmente sobre como en algun momento pueda que llegue a usar estos mismos conocimientos para mmi trabajo en ciberseguridad; El uso de grafos on solo resultó adecuado, sino esencial para comprender el comportamiento de la red, pues identificar nodos críticos fue vitar para evaluar el esfuerzo del ataque.