Karla Mondragón, A01025108

3 de diciembre 2021

Programación de Estructuras de Datos y Algoritmos Fundamentales

Jorge Rondríguez

Reflexión: Entrega Final Reto

Para la primera entrega del reto, trabajamos con métodos de búsqueda y ordenamiento, al igual que con la complejidad computacional de dichos métodos. Específicamente trabajamos con Merge Sort, búsqueda binaria y búsqueda secuencial. Durante esta entrega, aprendí cómo elegir entre métodos y funciones por medio de la optimización del código y cuáles son los costos computacionales de un código no eficiente.

En la segunda entrega del reto trabajamos con estructuras de datos, específicamente vectores, pilas y colas. Para las conexiones entrantes se usó stack ya que necesitamos una estructura que permita obtener la última conexión entrante y que permite leerlas desde la última a la primera. Para las conexiones salientes se utilizó queue debido a que deben de estar ordenadas desde la primera a la última, contrario a las conexiones entrantes. Se utilizó el vector para poder iterar. Aprender acerca de estas estructuras de datos me dió una perspectiva más amplia de las diferentes maneras que existen para analizar un mismo conjunto de datos; las pilas y las colas, aunque no las más eficientes para este reto abrió nuestro panorama acerca de qué era lo que estaba pasando y como las computadoras interactuaban.

Dentro de la tercera entrega utilizamos un diccionario de strings y de objetos de la clase ConexionesComputadora que creamos en la entrega anterior y hashes para poder determinar cuáles eran los dominios anómalos y cómo interactúan con el dominio de la situación problema. Los diccionarios fueron una de las estructuras de datos más útiles debido a que se pudo relacionar una llave (dirección IP o dominio del sitio) con la cantidad de conexiones, lo cual reveló parte del comportamiento de las computadoras.

Usamos árboles binarios y un diccionario en la entrega número 4 para poder ordenar los datos de acuerdo al nombre del dominio y la cantidad de conexiones entrantes, una vez que estaban ordenados, pudimos clasificarlos en un top 5 por fecha y entender su comportamiento e interacciones con otras direcciones IP. Las ventajas más importantes que nos dió el usar árboles, es que ordena automáticamente los datos y permite la relación entre las conexiones y el vector de los dominios por fecha.

En la última entrega del reto, clasificamos los datos que ya habíamos identificado (los dominios anómalos, la IP en la que se conectan las otras IPs, el sitio web con tráfico anómalo) y mediante grafos buscamos conexiones anómalas entre las IPs y dichos datos, hasta tener una teoría de que es lo que estaba pasando. Aprendimos conceptos como DDoS, Botmaster, cómo se infectaron y cuál era el propósito. Esta entrega fue la más

importante y es cuando aplicamos nuestro conocimiento a la realidad, analizando cómo es que las computadoras pueden ser infectadas, como infectan a otras y como es que pueden atacar.

Las estructuras más eficientes para poder terminar el reto con éxito fueron los diccionarios y los grafos ya que nos permitieron determinar algunos de los comportamientos más reveladores en este ataque, a los atacantes, los infectados y el método de infección.

Por último, considero que una representación visual de estas estructuras, específicamente de grafos, podría ser de gran utilidad, en una especie de tablero de tráfico y conexiones entrantes y salientes de nuestra red para poder visualizar el comportamiento de las IPs de manera más sencilla.