Gabriel Martínez Berrones A00517149

Reflexión sobre la actividad 3.4

La situación problema que se nos plantea es, utilizando los distintos tipos de algoritmos que hemos aprendido, lograr identificar cuál es el mejor y más eficiente de estos, para utilizarlo en la identificación de dispositivos que han sido infectados.

Las BST son una herramienta bastante poderosa ya que cuentan con una visualización más amigable a la vista, además de que cuenta con un tipo de priorización, que puede ser definida por nosotros o el usuario. En un caso de la vida real, este tipo de herramienta pudiera ser de gran ayuda para poder determinar que tarea se debe de realizar primero ya sea a nivel escolar o empresarial, siendo que a nivel escolar, la tarea que se encuentre en la cima de nuestro BST es la que mayor puntuación tiene y es la que debemos de realizar primero, o en el mundo empresarial, puede que la primera tarea sea la que nos deje un mayor número de ingresos. Y no solamente en situaciones diarias, sino que también en el aspecto tecnológico, y en el caso de nuestro reto, poder identificar si una red se encuentra infectada.

En esta entrega lo que se hizo fue, agrupar las IPs y obtener las 5 que contaran con el mayor número de registros, entonces, ¿esto cómo nos ayuda a identificar si una red está infectada? En el archivo bitácora contamos con 5 datos: día, hora, IP, puerto y motivo por el cual no se pudo accesar a la cuenta. Al momento de agrupar los datos como se hizo en esta evidencia, podemos tener a simple vista todos los registros que se realizaron de manera ordenada para así poder interpretarlos. Utilizando la fecha y la hora, podemos deducir si la red se encuentra infectada debido a un gran número de registros con acceso fallido en un corto periodo de tiempo. Además, sumando a esta información, podemos utilizar la IP y el puerto para identificar si estos intentos se están llevando a cabo desde una misma localización, lo cual nos puede indicar que existe un computador principal que está intentando acceder a las computadoras de la red de manera continua. Finalmente, existe el motivo de la falla, y este es probablemente el más importante ya que nos puede identificar si no se logró un ingreso por contraseña incorrecta por un usuario desconocido o “ilegal”, para el admin o desde uno de los computadores de la red.

Utilizando esta información y haciendo las implementaciones de un BST, donde podemos agrupar por fechas, registros, IP, etc., es sumamente sencillo lograr identificar si una red realmente se encuentra infectada o no.