Conceptos Básicos y Algoritmos Fundamentales

Actividad Integral de Grafos

Juan Carlos Garfias Tovar

A01652138

David Alonso Cantú Delgado

22 de noviembre del 2020

Reflexión

Los grafos son estructuras de datos sumamente relevantes en el mundo de la ciberseguridad y en la informática como tal. En este caso, se hace una lectura de todas las IPs y a partir de las conexiones se realiza el grafo. Este tipo de estructuras permiten conocer qué tipo de uniones, relaciones o conexiones tienen con otros nodos. Las estructuras de grafos debido a estas propiedades son sumamente útiles para todo tipo de ambientes, especialmente de aquellos donde se necesite conocer la interacción entre nodos. A partir de esta teoría no solo es posible conocer a nivel red las distancias entre nodos, sino que también permiten conocer grupos y a partir de algoritmos como kmeans es posible realizar análisis de datos altamente profunda.

Uno de los elementos mas importantes en la ciberseguridad es el uso de grandes cantidades de datos, en este caso la cantidad de registros es considerable por lo que la mejor eficiencia posible al momento de encontrar ocurrencias ayuda a que la velocidad y el coste computacional general sea menor que en una búsqueda simplemente secuencial. El poder implementar búsquedas rápidas con grafos y otras estructuras como heaps hacen de este problema algo directo y eficiente al momento de ser resuelto. Los nodos siendo la nace de las estructuras mas importantes son clave para almacenar información y permiten hacer uso de la IP como un key.

El uso de este tipo de estructura de datos es utilizado para poder obtener las rutas mas eficientes en mapas. Si en el node se ingresaran valores como coordenadas serias posible entonces también aplicar algoritmos como Dijkstra para poder encontrar las rutas con menor tiempo. Viendo un grafico de un mapa entre interacciones de las IPs a partir de las listas de adyacencia ayudaría a encontrar de manera visual y grafica los ataques mas recurrentes, zpnas de origen de estos ataques y encontrar grupos o zonas de alto peligro.

En aplicaciones de ciberseguridad es probable que los grafos puedan ser ocupados para conocer información de los usuarios, detectar a partir de distancias comportamientos sospechosos y también para poder ser utilizados en indexado y búsquedas con vínculos. En la actividad, esta estructura permitida mejorar considerablemente el tiempo para poder encontrar las ips sospechosas y dar a conocer esta información de manera eficiente, tanto en memoria como en tiempo de ejecución,