Tecnológico de Monterrey

Campus Santa Fe (CSF)

Programación de Estructura de Datos y Algoritmos

Actividad 5.2: Actividad Integral sobre el uso de diccionarios y conjuntos

Integrantes:

García Puebla Diego Fernando - A01028597

Serrano Diego Andrea - A01028728

Fecha de entrega: 28 de noviembre de 2021

Profesor: Nonell Cubells Vicente

Equipo: 7

Preguntas a resolver

1. ***Hay algún nombre de dominio en el conjunto que sea anómalo (Esto puede ser con inspección visual).***

   Sí, se puede observar que hay algún nombre de dominio en el conjunto, el cual es anómalo.

2. ***¿Cuál es su IP?, ¿Cómo determinarías esta información de la manera más óptima en complejidad temporal?***

   La dirección ip es *1.6.154.202*, con la inspección visual identificamos el nombre del dominio anómalo que es *3jb6992rz5rtdc2id9c5.net*, para encontrarlo creamos la función encontrarAnomalos(computadoras), le dimos como parámetros de búsqueda la longitud del dominio y caracteres no alfanuméricos.

   Una implementación óptima sería utilizar algún algoritmo de machine learning, que detecte dominios anómalos y los aprenda, la complejidad sería O(1).

3. ***De las computadoras pertenecientes al dominio reto.com determina la cantidad de IPs que tienen al menos una conexión entrante. (Recuerda que ya tienes la dirección de la red y el último octeto puede tener computadoras del .1 al .254. Imprime la cantidad de computadoras.***

   Hay 104 computadoras pertenecientes al dominio *reto.com* con al menos una conexión entrante.

4. ***Toma algunas computadoras que no sean server.reto.com o el servidor DHCP. Pueden ser entre 5 y 10. Obtén las IPs únicas de las conexiones entrantes.***

   172. 22.162.10

   172.22.162.2

   172.22.162.3

172.22.162.4

172.22.162.5

172.22.162.6

172.22.162.7

5. ***Considerando el resultado de las preguntas 3 y 4, ¿Qué crees que esté ocurriendo en esta red? (Pregunta sin código)***

   104 computadoras internas tienen conexiones entrantes. Esto significa que computadoras externas están intentando acceder a la información.

6. ***Para las IPs encontradas en el paso anterior, determina si se han comunicado con los datos encontrados en la pregunta 1.***

   Si la ip 172.22.162.212 que pertenece a server.reto.com tuvo conexiones con los sitios anómalos.

7. ***En caso de que hayas encontrado que las computadoras del paso 1 y 4 se comunican, determina en qué fecha ocurre la primera comunicación entre estas dos y qué protocolo se usa.***

   Sí, la fecha fue 17/08/2020 con el puerto 27203

Reflexión Personal

Los conjuntos nos permitieron identificar las computadoras, las ip y los nombres sin repetirlos, también para manejar las conexiones entrantes y salientes. Los diccionarios facilitaron identificar la información almacenada en cada variable de una forma más eficiente y guardarla para emplear los datos hacia nuestro objetivo de encontrar la computadora infectada y como fue contagiada.