Instituto Tecnológico y de Estudios Superiores de Monterrey

Programación de estructuras de datos y algoritmos fundamentales

Actividad 1.3

Presentan:

Ian Seidman Sorsby A01028650

Gianluca Beltran Binachi A01029098

ASESOR: Leonardo Chang

Campus Santa Fe ***Septiembre 2020***

1.- Hay algún nombre de dominio que sea anómalo (Esto puede ser con inspección visual).

Si, el nombre de dominio *249krwpsl2ciatl5u8nb.ru* es anómalo. También el dominio yjdcy2j66s4tk12hsa23.org es anómalo.

2.- De los nombres de dominio encontrados en el paso anterior, ¿cuál es su ip? ¿Cómo determinarías esta información de la manera más eficiente en complejidad temporal?

Para encontrar su ip se puede utilizar una búsqueda secuencial, que tiene la complejidad temporal más baja para los nombres de dominio que no están ordenados. Esta búsqueda tiene una complejidad temporal O(n) y se puede encontrar que el IP del dominio *249krwpsl2ciatl5u8nb.ru* es: 123.22.79.224 y la IP del dominio yjdcy2j66s4tk12hsa23.org es: 33.50.66.90.

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.

33 de las computadoras en el dominio reto.com tienen por lo menos una conexión entrante.

4.- Toma algunas computadoras que no sean server.reto.com o el servidor dhcp. Pueden ser entre 5 y 150. Obtén las ip únicas de las conexiones entrantes.

Se creó un set en el que insertamos todos los ip de conexión entrante que no son parte de server.reto.com o el servidor dhcp el cual tiene como puerto base 68 y puerto destino 67.

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

Creemos que está ocurriendo un ataque de bots ya que el número de conexiones a los ip anómalos es de 2492, un número relativamente alto.

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

Como dijimos anteriormente si se han comunicado las computadoras con los ips anómalos, 2492 veces para ser exactos.

Aportaciones:

Ian Seidman Sorsby: Yo realize la parte 1 del reto y las preguntas 1, 2 y 3. Esto incluye el conjunto de strings para guardar los nombres que no pertenecen a reto.com y los métodos necesarios para contestar las preguntas 1,2 y 3 dentro de analytics.cpp y act.cpp.

Gianluca Beltran Bianchi: Yo me encargue de la parte 2 del reto y también de las preguntas 4 a 6. Cree el diccionario con el nombre del host y el objeto de las conexiones asi como el codigo para contestar las preguntas 4 y 6.