Reporte Avance de Reto 5

Tomas Diaz Servin A01637531

Isaac Husny Tuachi A01027140

Programación de estructuras de datos y algoritmos fundamentales (Gpo 100)

Prof. Jorge Rodriguez Ruiz

En los retos pasados encontraste la siguiente información:

1. Una ip interna, que llamaremos A, la cual se comunica con algunas otras computadoras internas.

   A: 172.31.90.47 :: kathleen.reto.com

2. Algún sitio con nombre raro, denominaremos B.

   B: 110.174.125.114 :: 916t95wtls6d3sie7ew6.net

3. Un sitio web normal que tiene un volumen de tráfico anómalo un día, el cual denominaremos C.

   C: 68.120.112.100 :: craigslist.com

En este reto vamos a trabajar en encontrar la cantidad de computadoras que se han conectado a estos sitios/ips. Para ello tienes que resolver las siguientes preguntas:

1. Utilizando un grafo con las conexiones entre las ip de la red interna, determina la cantidad de computadoras con las que se ha conectado A por día. ¿Es el vértice que más conexiones salientes hacia la red interna tiene?

   Es el vértice que tiene más conexiones salientes hacia la red con un promedio de 48.71 conexiones con computadoras dentro de la red por día.

   Código encontrado en Reto Avance5.cpp.

2. Utilizando el grafo del punto anterior, ubica la cantidad de computadoras que se han conectado hacía A por día. ¿Existen conexiones de las demás computadoras hacía A?

   En la red interna, cada una de las **31 computadoras** que forman parte de la red se han conectado hacia la IP de kathleen.reto.com (712.31.90.47).

   Código encontrado en Reto Avance5.cpp.

3. Utilizando un grafo de conexiones a sitios web, determina cuántas computadoras se han conectado a B por día.

   Después del día 14 de agosto, solamente una computadora se ha conectado hacia el sitio B.
   Código encontrado en Reto Avance5.cpp.

4. Utilizando el mismo grafo del punto anterior, indica cuántas computadoras se han conectado a C por día.

   Es importante notar que el día del ataque (19 de agosto) se conectaron 31 computadoras de la red interna.

   Código encontrado en Reto Avance5.cpp.

5. (Pregunta sin código): Investiga que es un ping sweep, un DDoS, un servidor de comando y control y un botmaster. ¿Ves estos elementos en tus datos?

- **Ping sweep** se refiere a una técnica de escaneo de redes la cual consiste en mandar una señal a todas las computadoras de una red y analizar cuales responden y cuáles no.
- **DDoS (distributed denial of service)**, es un tipo de ataque cibernético donde el atacante intenta hacer un número de conexiones a un servidor mayores a las que el servidor puede soportar.
- Un servidor de **comando y control** es aquella computadora que es infectada con malware con el propósito de infectar a más computadoras dentro de la red de esta misma.
- El **botmaster** puede ser descrito como el parent de los servidores de comando y control. Este es el servidor del atacante buscando computadoras para infectar con malware y así convertirlos en servidores de comando y control.

Analizando nuestro código y los resultados podemos llegar a la conclusión que se llevó a cabo un **ataque de DDoS sobre el sitio craigslist.org**. El dominio **916t95wtls6d3sie7ew6.net** se trata de un **servidor comando control y botmaster** que únicamente tiene conexiones entrantes por parte de kathleen.reto.com. Luego, utilizando un ping sweep y localizando las demás computadoras dentro de la red, el botmaster le da instrucciones para infectar a las demás computadoras de la red, y finalmente las utiliza para realizar el ataque el día 19 de agosto.