



**Tecnológico
de Monterrey**

Campus Santa Fe

Escuela de Ingeniería y Ciencias

Avenida: Computación y Tecnologías de la Información

TC1031.101

Programación de Estructuras de Datos y Algoritmos Fundamentales

Docente: Dr. Leonardo Chang Fernández

Act/Reto 5 - Actividad Integral de Grafos (Evidencia Competencia)

Axel Mercado Gasque

A00829051

Fecha de entrega: 26 de noviembre del 2020

En los retos pasados encontraste la siguiente información:

1. Una ip interna, que llamaremos *A*, la cual se comunica con algunas otras computadoras internas.
2. Algún sitio con nombre raro, al cual denominaremos *B*.
3. Un sitio web normal que tiene un volumen de tráfico anómalo en un día, el cual denominaremos *C*.

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:

Nota: Para contestar las siguientes preguntas se tomará *A* como la dirección IP **172.31.224.103**

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 *A* el vértice que más conexiones salientes hacia la red interna tiene?

Fecha	Número de IP internos con los que se conecta A
10-8-2020	1
11-8-2020	1
12-8-2020	1
13-8-2020	1
14-8-2020	2
17-8-2020	2
18-8-2020	2
19-8-2020	2
20-8-2020	2
21-8-2020	2

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

Fecha	Número de IP internos que se conectan con A
-------	---

10-8-2020	0
11-8-2020	0
12-8-2020	0
13-8-2020	0
14-8-2020	1
17-8-2020	0
18-8-2020	0
19-8-2020	1
20-8-2020	0
21-8-2020	0

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

Fecha	Número de dominios que se conectan con el dominio "li44wsvsoyx7vukfvuu5.xxx"
10-8-2020	0
11-8-2020	0
12-8-2020	0
13-8-2020	0
14-8-2020	1
17-8-2020	0
18-8-2020	0
19-8-2020	0
20-8-2020	0
21-8-2020	0

Fecha	Número de dominios que se conectan con el dominio "lnrar56w11linjvv5bnj.net"
10-8-2020	0
11-8-2020	0
12-8-2020	0
13-8-2020	0
14-8-2020	1
17-8-2020	1
18-8-2020	1
19-8-2020	1

20-8-2020	1
21-8-2020	1

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

Fecha	Número de dominios que se conectan con el dominio "protonmail.com"
10-8-2020	34
11-8-2020	34
12-8-2020	34
13-8-2020	34
14-8-2020	34
17-8-2020	34
18-8-2020	34
19-8-2020	34
20-8-2020	34
21-8-2020	34

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 hace referencia a un método para descubrir dispositivos conectados en una red. De tal manera, sí se observa este elemento en los datos ya que se ingresa una dirección IP perteneciente a la red interna y se aplica un algoritmo para determinar si se conecta con otros dispositivos o bien si otros dispositivos se conectan con esta dirección.

No se cuenta con suficiente información para determinar si hay un Ddos en los datos, ya que no se puede determinar si el dominio anómalo está deteniendo de alguna manera el funcionamiento de la red.

De igual manera no se encuentran en los datos un servidor de control y comando ni un botmaster. Un servidor de control y comando hace referencia a un computador que da indicaciones a dispositivos infectados con malware, y no se observa en los datos. De manera similar, un botmaster es una persona encargada de administrar y programar un chatbot, lo que tampoco se observa en los datos.