Tecnológico de Monterrey

Campus Santa Fe

ALUMNOS:
Yarezzi Garcia, A01653133
Octavio Fenollosa, A01781042
Diego Araque, A01026037

PROFESOR:
Jorge Rodriguez

MATERIA:
Programación de estructuras de datos y algoritmos fundamentales

GRUPO:
101

Reto 5

FECHA DE ENTREGA:
Noviembre de 2021

A- 172.24.133.84, debra.reto.com

B- 213.197.181.214, 3ynvanote9acan4yaffn.com

C- bankofamerica.com, 68.76.127.243

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?**

   La computadora de debra.reto.com solo se conecta con otras computadoras en la fecha 14-8-2020 y en la fecha 19-8-2020.

   En la 14-8-2020 se conecta con 34 computadoras y con cada una 2 veces. Mientras que en la 19-8-2020 se conecta a 33 computadoras 1 sola vez.

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 ningún día existen conexiones hacia la computadora de debra.

3. **Utilizando un grafo de conexiones a sitios web, determina cuántas computadoras se han conectado a *B* por día.**
4. **Utilizando el mismo grafo del punto anterior, indica cuántas computadoras se han conectado a *C* por día.**

```
10-8-2020
Las conexiones B son :0
Las conexiones C son :9
~/Reto5$ g++ main.cpp
~/Reto5$ ./a.out
11-8-2020
Las conexiones B son :0
Las conexiones C son :11
~/Reto5$ g++ main.cpp
~/Reto5$ ./a.out
12-8-2020
Las conexiones B son :0
Las conexiones C son :8
~/Reto5$ g++ main.cpp
~/Reto5$ ./a.out
13-8-2020
Las conexiones B son :0
Las conexiones C son :7
~/Reto5$ g++ main.cpp
~/Reto5$ ./a.out
14-8-2020
Las conexiones B son :1
Las conexiones C son :9
~/Reto5$ g++ main.cpp
~/Reto5$ ./a.out
17-8-2020
Las conexiones B son :1
Las conexiones C son :13
```

```
18-8-2020
Las conexiones B son :1
Las conexiones C son :9
~/Reto5$ g++ main.cpp
~/Reto5$ ./a.out
19-8-2020
Las conexiones B son :1
Las conexiones C son :34
~/Reto5$ g++ main.cpp
~/Reto5$ ./a.out
20-8-2020
Las conexiones B son :1
Las conexiones C son :7
~/Reto5$ g++ main.cpp
~/Reto5$ ./a.out
21-8-2020
Las conexiones B son :1
Las conexiones C son :8
```

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: (ICMP Sweep) Consta de un ataque o escaneo a un rango de direcciones IP de una red, en el cual se buscan " live hosts" a los cuales conectarse para probar vulnerabilidades en ellos y en la red. Funciona mandando "pings" a cada uno de los ordenadores. En el reto podemos ver que la computadora de debra está actuando como Ping Sweep, porque después de ser infectada esta computadora se conecta a otras para infectarlas.

DDoS: Los ataques DDoS están diseñados para deshabilitar servidores, servicios o infraestructura. Se envían múltiples solicitudes al recurso web atacado. El propósito es saturar la capacidad del sitio web para manejar múltiples solicitudes y evitar que el sitio web funcione con normalidad. Esto sucede en la red cuando el dia 19 la computadora de debra se

conecta a los live hosts para que estos se conecten con la ip de bank of america ya que esa fue la que detecto un nivel de tráfico anómalo ese dia.

Servidor de Control-Comando: Se trata de un servidor que controla y está conectado a los dispositivos que estén infectados con su malware, recibe información de estos dispositivos al igual puede ordenar que se duplique y se propague el mismo malware. Algunos servidores controlan millones de dispositivos. La computadora de debra igualmente actúa como servidor de control comando, ya que ésta computadora manda las acciones a las otras ips para atacar.

Botmaster (Bot Herder): Controlador de una botnet, se trata de bots remotos que se ejecutan de manera autónoma y automática, funciona mandando ataques contra servidores o redes. En nuestro archivo se observa con la ip anómala, que es la que se conecta a la computadora de debra y genera el virus.

Conclusiones:

Diego: En este reto aprendimos sobre una de las estructuras más importantes y útiles de nuestro dia a dia. Al no ser una librería de STL cambiamos las funciones hechas en clases, para que de esa manera se ajustará a lo que buscábamos hacer. Lo que más nos costó fue recorrer el grafo, ya que nos confundimos bastante al no ser una librería STL. Pero al final con ayuda del profesor, pudimos generar la función y recorrer el grafo perfectamente. Fue muy interesante ver el producto final de todas las otras entregas que hicimos en el semestre y entender cómo la red estaba infectando y que estaba sucediendo.

Yarezzi: Durante el desarrollo del reto pude comprender de una mejor manera los grafos, al igual que comprendí la importancia de los grafos, pues se usan para las conexiones de internet, por lo que podemos decir que son aspectos con los que interactuamos a diario. Durante el reto pude aportar soluciones para realizar las preguntas solicitadas, como calcular la cantidad de conexiones que se conectan a C y D, al igual que pude aportar a la creación de grafos.

Octavio: En el desarrollo de este reto usamos una de las estructuras más usadas e importantes llamada grafos, esta se utiliza en nuestro dia a dia mas que nada en conexiones a internet. Al no tener librería nos encontramos con algunos problemas al momento de usarlos, pero después de investigar y con la ayuda del profesor pudimos resolverlos cambiando las funciones que teníamos, para poder identificar las distintas conexiones realizadas en la red y cómo se comportan las anómalas. En donde más aporte fue en la investigación de los distintos tipos, al igual que las modificaciones necesarias al grafo que habíamos hecho en la clase junto con mi equipo.

Mezquita, T. (2020, 8 mayo). *Bot, Botnet, Bot Herder, and Bot Master*. CyberHoot.

https://cyberhoot.com/cybrary/bot-botnet-bot-herder-and-bot-master/

Informe, D. (2021, 4 mayo). *¿Qué es un servidor de comando y control para malware?* Diario Informe. https://diarioinforme.com/que-es-un-servidor-de-comando-y-control-para-malware/