Instituto Tecnológico y de Estudios Superiores de Monterrey

Programación de estructuras de datos y algoritmos fundamentales

Grupo 100

"Reto 5 - Actividad Integral de Grafos (Evidencia Competencia)"

Profesor: Jorge Rodriguez

Alumno:

Fernanda Nava Moya - A01023896
Sebastion Juncos - A01022629

- **brian.reto.com 172.26.185.121 (*A*):** Una ip interna, la cual se comunica con algunas otras computadoras internas.
- **x42olekrcpb929dv2iwn.xxx (*B*):** Algún sitio con nombre raro.
- **nytimes.com (*C)***: Un sitio web normal que tiene un volumen de tráfico anómalo un día.

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?**

   Tiene 254 conexiones, y si es la computadora con más conexiones salientes, además de que es la única computadora que se comunica con otras dentro de la red interna.

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 hacia A?**

   No existen otras computadoras que se conecten a la computadora A (172.26.185.121), solamente se conectó esta misma computadora a si misma.

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

   Solo una, la computadora A (172.26.185.121)

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

   10-8-2020: 11
   11-8-2020: 9
   12-8-2020: 11
   13-8-2020: 14
   14-8-2020: 12
   17-8-2020: 320
   18-8-2020: 9
   19-8-2020: 9
   20-8-2020: 10
   21-8-2020: 15

5. **(Pregunta sin codigo): 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
    - Es un sistema que identifica si un host está vivo dentro de una red interna a través de sus IPs. Cuando un host está vivo, este regresa un 1; cuando un host está muerto, regresa un 0
    - El ping sweep no lo utilizamos, ya que no vemos si la computadora está viva o no, pero sería una buena idea el implementarlo para buscar bots
- DDoS
    - Un Distributed Denial-of-Service Attack (ataque DDoS) es un tipo de ataque que altera el tráfico regular en un servidor o red al abrumar el tráfico en la red.
    - Si hay un DDoS al nytimes.com ya que la cantidad de tráfico proveniente de una computadora de la red interna en específico en un día es demasiado grande.

- Servidor de Comando y Control (C&C o C2)
    - Es un computador que dicta órdenes a dispositivos infectados con malware y recibe información de estos. Un computador puede controlar millones de dispositivos.

- Botmaster
    - Es una persona que opera el comando y control de botnets (colección de computadoras comprometidas o computadoras "zombies"), esta persona ocultara su dirección IP para poder obtener información, hackear credenciales de botnets o incluso robar los botnets de otro botmaster.
    - En nuestros datos el botmaster es el sitio de nombre **x42olekrcpb929dv2iwn.xxx** cuya ip es **210.210.126.3**

Referencias APA

- Ping Sweep: Definition, Tools & Uses. (s.f.). Retirado en Noviembre 26, 2010, de https://study.com/academy/lesson/ping-sweeps-definition-tools-uses.html#:~:text=Ping%20Sweep%20is%20a%20technique,network%20with%20network%20ID%20192.10.
- Servidor de Control y Comando. (s.f.). Retirado en Noviembre 26, 2020, desde https://ssd.eff.org/es/glossary/servidor-de-control-y-comando
- Radware. (s.f.). DDoS Attack Definitions - DDoSPedia. Retirado en Noviembre 26, 2020, desde https://security.radware.com/ddos-knowledge-center/ddospedia/botmaster/, https://security.radware.com/ddos-knowledge-center/DDoSPedia/botnet/
- What is a DDoS Attack?. (s.f.). Retirado en Noviembre 26, 2020 de https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/