Lourdes Badillo, A01024232
Eduardo Villalpando, A01023646
Programación de Estructuras de Datos y Algoritmos Fundamentales
Profesor Leonardo Chang

Reporte

I. 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.

10/8/2020: 1
11/8/2020: 1
12/8/2020: 1
13/8/2020: 1
14/8/2020: 1
17/8/2020: 287
18/8/2020: 1
19/8/2020: 32
20/8/2020: 1
21/8/2020: 1

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

10/8/2020: No
11/8/2020: No
12/8/2020: No
13/8/2020: No
14/8/2020: No
17/8/2020: Sí
18/8/2020: No
19/8/2020: Sí
20/8/2020: No
21/8/2020: No

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?

17/8/2020: 2
19/8/2020: 1

Sí existen conexiones entrantes a la computadora con IP: 172.26.89.118

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

10/8/2020: 0

11/8/2020: 0

12/8/2020: 0

13/8/2020: 0

14/8/2020: 0

17/8/2020: 1

18/8/2020: 0

19/8/2020: 0

20/8/2020: 0

21/8/2020: 0

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

10/8/2020: 8

11/8/2020: 6

12/8/2020: 7

13/8/2020: 6

14/8/2020: 10

17/8/2020: 8

18/8/2020: 12

19/8/2020: 402

20/8/2020: 7

21/8/2020: 14

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

Un ping sweep (o barrido de puertos) es un ataque que envía peticiones “ping” a un rango de direcciones IP, teniendo como objetivo el encontrar hosts y probarlos en busca de vulnerabilidades. (*Ping Sweep*, n.d.)

Un DDoS (ataque de denegación distribuida de servicio) es un tipo de ataque que aprovecha los límites de capacidad que tiene un recurso de red. El DDoS envía múltiples solicitudes al recurso atacado, con la intención de desbordar su capacidad y por lo tanto, deje de funcionar correctamente. (Kaspersky, n.d.)

Un servidor de control y comando es una computadora que manda órdenes a dispositivos infectados con malware, permitiéndole recibir información de estos. (Electronic Frontier Foundation, n.d.)

Un botmaster es una persona que opera un servidor de control y comando. (Radware, n.d.)

Sí, la computadora de Jennifer fue infectada por malware el 17 de agosto, cuando se conectó al sitio anómalo por medio del puerto 443.

Ese mismo día, la computadora de Jennifer se conectó a 287 computadoras en la red interna, lo que podría indicar que se realizó un **ping sweep**.

A partir de entonces puede observarse que la misma computadora realizaba solicitudes diarias a la dirección anómala. Esto puede indicar que se realizó un ataque **DDoS**.

Por lo tanto, puede identificarse que un **botmaster** usaba un **servidor de control y comando** para mandar las instrucciones a las computadoras infectadas.

II. Aportaciones

Para poder realizar este entregable, nos dividimos las diferentes tareas de la siguiente forma:

Tarea	**Responsable**
Realizar implementación de clase de Grafos	Lourdes
Realizar método para iterar por todas las fechas y añadir nodos a grafos	Eduardo
Agregar arcos correspondientes por día al grafo de conexiones internas	Lourdes
Implementar método para añadir arcos usando valores en vez de índices	Eduardo
Realizar mapas de conexiones salientes y conexiones entrantes por día para la red interna	Lourdes
Realizar método para obtener el ip con mayor cantidad de conexiones diarias	Eduardo
Realizar método para comprobar si la ip corresponde con el mayor del día	Lourdes
Implementar método para poblar grafos de sitios web	Eduardo
Investigación sobre pregunta 5	Lourdes

Bibliografía

Electronic Frontier Foundation. (n.d.). *Servidor de Control y Comando*. SURVEILLANCE SELF-DEFENSE. https://ssd.eff.org/es/glossary/servidor-de-control-y-comando

Kaspersky. (n.d.). *¿Qué son los ataques DDoS?* Kaspersky Latinoamérica. https://latam.kaspersky.com/resource-center/threats/ddos-attacks

Ping Sweep. (n.d.). Glosario Terminología Informática. http://www.tugurium.com/gti/termino.php?Tr=ping%20sweep

Radware. (n.d.). *Botmaster*. DDoS Attack Definitions - DDoSPedia. https://security.radware.com/ddos-knowledge-center/ddospedia/botmaster/#:~:text=A%20botmaster%20is%20a%20person,forms%20of%20remote%20code%20installation