Reflexión Act 4.2

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?

No, no es el vertice que más conexiones salientes tiene.

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?

Si, existen tres conexiones de las demás computadoras hacia A.

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

Al sitio de nombre raro solo hubieron tres conexiones en dos diferentes días.

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

Se conectan menos de 20 computadoras a C por día, excepto un día que tiene 543 conexiones.

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

Un ping sweep es una técnica para encontrar entre muchas direcciones IP, cuáles están conectadas en ese momento a una computadora anfitriona. SI se encuentra un ping sweep en nuestros datos, porque todo el análisis que estamos haciendo al archivo y a las direcciones IP podría ser un ping sweep.

Un DDoS (Distributed denial-of-service attack) es un intento para afectar el tráfico que recibe un servidor o una red. Esto se logra dirigiendo grandes cantidades de tráfico al objetivo. El sitio web que recibe una cantidad de coexiones anómala en un día tiene características de un DDoS.

Un servidor de comando y control es una computadora que da órdenes a dispositivos infectados con malware y recibe información de ellos. Podría ser el sitio con nombre raro o el sitio que recibe muchas conexiones en un día.

Un botmaster es una persona que controla las botnets desde un lugar remoto y con su identidad protegida. Si hay un DDoS y un servidor comando y control, probablemente hay un botmaster haciendo esas acciones.

División de trabajo: Yo, Iñigo, hice el grafo para las primeras dos preguntas y las funciones para contestarlas. Andrés hizo el grafo para las preguntas 3 y 4, y las funciones para contestarlas.