Ana Paula Katsuda, A01025303
Andreína Sanánez, A01024927
Programación de estructuras de datos
Prof. Jorge Rodríguez
30 de Noviembre 2021

# Reporte Reto 5

**Introducción**

Analizar y procesar información sobre distintas interacciones de usuarios con distintos servicios en la computación, es inmensamente importante para identificar si existen accesos maliciosos en redes y proteger datos relevantes. Los accesos maliciosos tienen la posibilidad de afectar enormemente a empresas e individuos; puede costar la privacidad de éstos, e incluso puede tener impactos monetarios significativos.

Considerando la relevancia de dar seguimiento a distintas interacciones, la finalidad del presente reporte es extender el análisis de interconexiones entre usuarios de la compañía “reto.com” consigo mismos y con servicios externos. Mediante el uso de grafos, será posible revisar con mayor detalle las conexiones del usuario “karen.reto.com” denominado como “A”, de “p7necksgkbynlvmgenv5.org” denominado como “B”, y de “wiktionary.com” denominado como “C”.

En específico, se quiere indagar en: las conexiones entre los ips internos por día (de tal manera que se identifique el comportamiento de A”), y las conexiones que se hacen por día tanto a B como a C.

**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?***

A partir de los grafos de matrices de adyacencia obtenidos es posible identificar que la única ip de la red interna que se conecta a otras ip internas, es la de A. Por lo tanto, sí es el vértice que tiene más conexiones salientes hacia 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?***

Visualizando nuevamente las matrices generadas a partir del grafo,, se vuelve notorio que la única computadora que se conecta hacia A, es A. Por ende, no existen conexiones de las demás computadoras hacia A. Es relevante mencionar que para los incisos 1 y 2 se decidió utilizar grafos implementados con matrices dado que la visualización de éstas se consideró más sencilla.

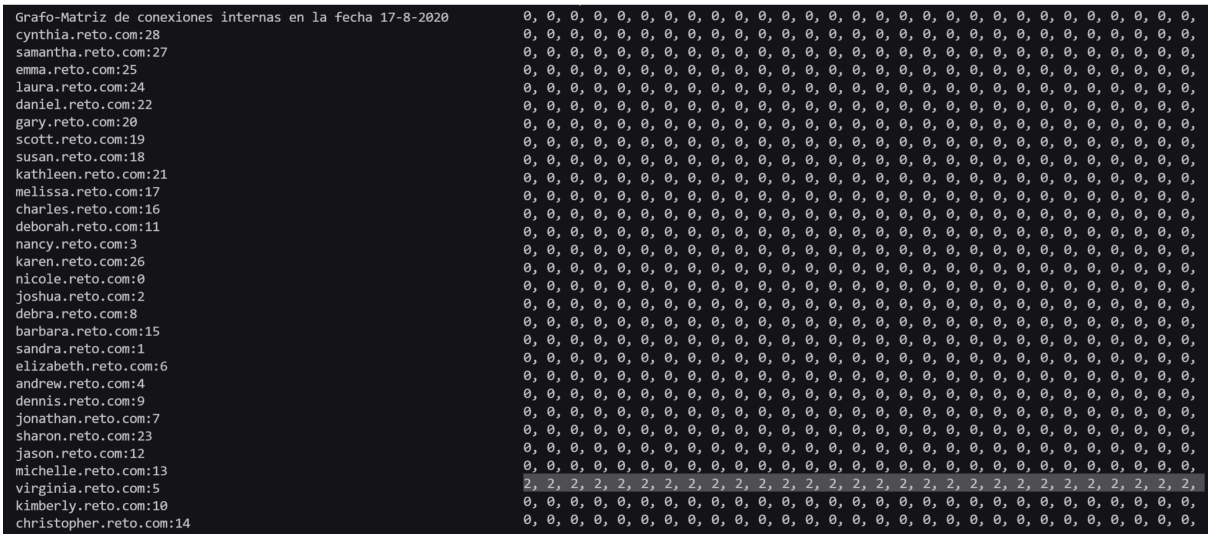


Figura 1. Matriz de adyacencia de las conexiones internas en la fecha 17-8-2020

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

A continuación se muestran las computadoras que se han conectado a B a partir del primer día en el que se tienen accesos maliciosos (en este caso 17-8-2020).
Es evidente que todas las computadoras de la empresa (29 usuarios) se conectaron a B.

De forma similar, es relevante notar cómo es que el dominio “karen.reto.com” (A) a comparación de las demás computadoras internas, tiene una gran cantidad de conexiones con el dominio anómalo “p7necksgkbynlvmgenv5.org”.

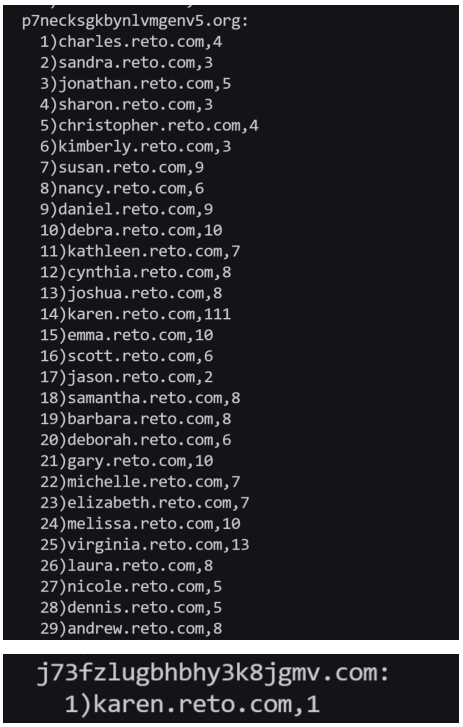


Figura 2. Lista de conexiones a sitios anómalos el 17-8-2020


Figura 3. Lista de conexiones a B 18-8-2020

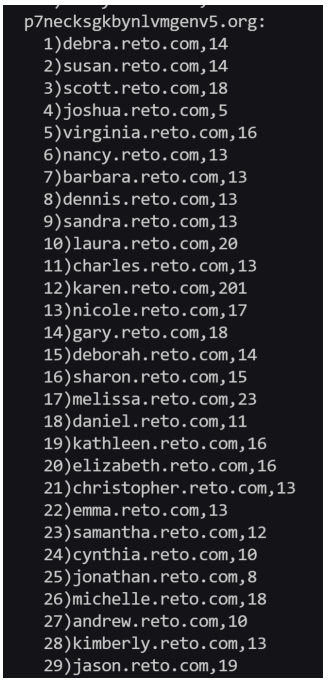


Figura 4. Lista de conexiones a B el 19-8-2020


Figura 5. Lista de conexiones a B el 20-8-2020


Figura 6. Lista de conexiones a B el 21-8-2020

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

En este caso, es posible observar que C recibe conexiones de los 29 usuarios pertenecientes a la empresa el día 18-8-2020. Los demás días, este Sitio Web tiene significativamente menos recepciones de conexiones por parte de los dominios de la

compañía (esto se ejemplifica en la Figura 7). Cabe mencionar que para los incisos 3 y 4 se decidió utilizar grafos de listas ya que éstos permiten una mejor visualización de las conexiones realizadas entre fuentes y destinos. Específicamente, la matriz tendría un gran cantidad de datos por lo que su interpretación sería más complicada.


Figura 7. Lista de conexiones a C el 18-8-2020


Figura 8. Lista de conexiones a C el 21-8-2020

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*: Es una técnica que se utiliza para determinar si los “hosts” o computadoras pertenecientes a cierta dirección IP se encuentran vivas. Específicamente esto se realiza mediante “echo requests” donde se entabla una conexión con cierta computadora y si esta responde (echo reply) significa que está viva.

- *DDoS*: Sus siglas hacen referencia al ataque de denegación de servicio distribuido. Este ataque consta de inundar el tráfico de internet de algún sitio con el fin de evitar que los usuarios del mismo puedan utilizar su servicio. Para lograr lo anterior, la

persona que desea efectuar dicho ataque malicioso requiere construir una red de computadoras (botnet) de la cual el mismo tenga control, para así poder saturar el tráfico de internet de dicho servicio que quiere denegar. Esto lo hace por medio de malware donde el atacante tiene la capacidad de controlar a las computadoras infectadas remotamente. Algunas maneras de identificar estos ataques es notando si existen cantidades sospechosas de conexiones provenientes de una sola dirección IP o si existe un aumento considerable de solicitudes de conexión a un servidor.

- *Servidor de comando y control:* el servidor de comando y control se refiere a una computadora controlada de manera remota por un usuario malicioso para enviar instrucciones a dispositivos que fueron infectados con malware (Mezquita, T., 2020). Dicho servidor puede ser externo a la red a la que se quiere atacar o puede estar instalado en una computadora interna que contribuye a mandar las señales a dispositivos.

- *Botmaster*: se denomina botmaster a la entidad que origina la botnet (red de computadoras comprometidas). Se refiere al individuo que controla toda la red de manera remota (utilizando el servidor de comando y control, por ejemplo).

Relacionando todo lo anterior a la presente problemática, es posible notar cómo es que en este caso comenzando con el dominio “karen.reto.com”, las computadoras de la compañía analizada fueron infectadas por el atacante detrás del dominio anómalo “p7necksgkbynlvmgenv5.org” para posteriormente utilizar las mismas para bombardear al sitio wikitionary.org con conexiones. En otras palabras, es posible relacionar cómo es que el comportamiento de las conexiones del reto se asemeja a aquel de un ataque DDos, en el cual las computadoras internas de la compañía forman parte del botnet del atacante.

Dicho esto, de la misma manera los demás términos explicados anteriormente se encuentran implícitamente relacionados con el ataque. Por ejemplo, es posible identificar que el dominio anomalo “p7necksgkbynlvmgenv5.org” es el botmaster el cual controla a todas las computadoras de la compañía. Asimismo, es notorio que este posiblemente utiliza la computadora de “karen.reto.com” como parte del servidor de comando y control, (considerando el gran número de conexiones pertenecientes a “karen.reto.com” con el dominio anómalo) ya que es a partir de este domino que las demás computadoras internas se infectan.

Finalmente, es relevante mencionar que el ping sweep, en este caso, pudo haber sido utilizado por el agente malicioso para verificar la vida de las computadoras pertenecientes a la red interna de la compañía, y así identificar a quiénes enviarles el malware.

**Aportaciones Individuales**

En cuanto a las aportaciones, es importante mencionar que el análisis de la situación problema, así como su resolución fue hecha en conjunto por las dos integrantes del equipo. Si bien ciertas actividades fueron realizadas de manera individual, se tuvieron varias sesiones de revisión para verificar el correcto funcionamiento de la incorporación de cada una de las aportaciones. A continuación, se mencionan las divisiones de tareas realizadas por cada integrante:

En conjunto:

- Análisis del problema.
- Pruebas del funcionamiento del código y de cada uno de los incisos.
- Reporte
    - Investigación de conceptos

Andreína Sanánez / A01024927:

- Implementación del grafo matriz

Ana Paula Katsuda / A01025303:

- Implementación del grafo vector

**Referencias**

Ataque de denegación de servicio (ataque DDoS). (s.f). *Cloudflare*. [Sitio Web]. Recuperado de: https://www.cloudflare.com/es-es/learning/ddos/what-is-a-ddos-attack/

Hanna, K. (2021, June 18). What is a ping sweep (ICMP sweep)? [Sitio Web] Recuperado de: https://www.techtarget.com/searchnetworking/definition/ping-sweep-ICMP-sweep

Mezquita, T. (2020). Command and Control (C&C) Server. CyberHoot. [Sitio Web]. Recuperado de: https://cyberhoot.com/cybrary/command-and-control-cc-server/

What is a DDoS Botnet. (s.f.) Imperva. [Sitio Web]. Recuperado de: https://www.imperva.com/learn/ddos/botnet-ddos/