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

Reporte Reto 3

Introducción

Recopilar información sobre las interacciones de los usuarios con distintos servicios, es de crucial importancia 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.

Dada la importancia de dar seguimiento de dichas interacciones, el objetivo del presente escrito es continuar con el análisis de las interacciones de los usuarios pertenecientes a la empresa “reto.com” con servicios externos a ella. En este caso, se expandirá lo realizado con las conexiones tanto entrantes como salientes y se hará un análisis de dominios anómalos mediante el uso de hash y diccionarios.

1. *Hay algún nombre de dominio que sea anómalo (Esto puede ser con inspección visual).*

Con el fin de identificar los dominios anómalos, lo primero que se hizo, fue buscar dominios que no incluyeran “reto.com”. Lo anterior se realizó mediante el uso de comparaciones con “string::npos” (esto está referenciado en el código).

```
mayoclinic.org
craigslist.org
nytimes.com
genius.com
forbes.com
p7necksgkbynlvmgenv5.org
amazon.com
allrecipes.com
fb.com
cbssports.com
instagram.com
lowes.com
```

```
urbandictionary.com
j73fzlugbhbhy3k8jgmv.com
groupon.com
pinterest.com
walmart.com
steamcommunity.com
play.google.com
mapquest.com
twitter.com
yelp.com
linkedin.com
```

Al ver los dominios mostrados anteriormente, es posible encontrar dos anómalos: p7necksgkbynlvmgenv5.org y j73fzlugbhbhy3k8jgmv.com.

2. *Del los nombres de dominio encontrados en el paso anterior, ¿cuál es su ip? ¿Cómo determinarías esta información de la manera más óptima en complejidad temporal?*

Retomando que en la pregunta anterior se determinaron los dominios anómalos p7necksgkbynlvmgenv5.org y j73fzlugbhbhy3k8jgmv.com, la dirección IP de estos se encontraron mediante la implementación de un diccionario (donde la llave es el nombre y el valor la IP) el cual se llenó con las mismas iteraciones necesarias para crear el “hash” solicitado. Se decidió realizar lo anterior, ya que de esta manera no solo se aprovechaba un ciclo que inevitablemente se debía de realizar, sino que además la acción de buscar dichas operaciones mediante un diccionario se logró con una complejidad temporal de O(1).

Asimismo, cabe mencionar que de no utilizar un diccionario se debían de realizar dos búsquedas, y de no utilizar búsqueda secuencial se debía de efectuar cierto tipo de ordenamiento.

A continuación, se encuentra una captura de pantalla con las direcciones IP para cada uno de los dominios anómalos encontrados.

```
IP de p7necksgkbynlvmgenv5.org: 220.218.191.76
IP de j73fzlugbhbhy3k8jgmv.com: 71.43.144.111
```

3. *De las computadoras pertenecientes al dominio reto.com determina la cantidad de ips que tienen al menos una conexión entrante. (Recuerda que ya tienes la dirección de la red y el último octeto puede tener computadoras del .1 al .254. Imprime la cantidad de computadoras.*

Al realizar el conteo de las computadoras de la compañía que tienen por lo menos una conexión entrante, se encontró lo siguiente:

```
Número de computadoras pertenecientes al dominio reto con por lo menos una conexión entrante: 254
```

4. *Toma algunas computadoras internas que no sean server.reto.com o el servidor dhcp. Obtén las ip únicas de las conexiones entrantes.*

Para las IP únicas de las conexiones entrantes, se eligió analizar las computadoras de Charles, Jason y Sharon (dominios con “reto.com”). En este caso, se encontró que todos estos usuarios tienen conexiones entrantes por parte del IP 172.24.238.38 (que pertenece a Karen) como se muestra a continuación:

```
Conexiones entrantes de charles.reto.com
172.24.238.38

Conexiones entrantes de jason.reto.com
172.24.238.38

Conexiones entrantes de sharon.reto.com
172.24.238.38
```

5. *Considerando el resultado de las preguntas 3 y 4, ¿Qué crees que esté ocurriendo en esta red? (Pregunta sin código)*

Dado que todas las computadoras que inicializan la conexión tienen por lo menos una conexión entrante, es posible inferir que existen comunicaciones entre dos computadoras internas (dos computadoras con dominio “reto.com”). En específico, se están conectando con la computadora de IP 172.24.238.38 (Karen). A partir de lo anterior, se cree que la computadora 172.24.238.38 tuvo una conexión maliciosa que adquirió acceso a la computadora interna de Karen y, mediante esta, se está intentando expandir a todas las computadoras de la red.

6. *Para las ips encontradas en el paso anterior, determina si se han comunicado con los datos encontrados en la pregunta 1.*

En efecto, el IP 172.24.238.38 perteneciente a Karen, sí se comunica tanto con p7necksgkbynlvmgenv5.org como con j73fzlugbhbhy3k8jgmv.com. Es posible observar esto a continuación:

```
Comunicaciones entre la IP 172.24.238.38 y los dominios anónimos:  (El primer Record es el que tiene la fecha más reciente)
17-8-2020,13:0:54,172.24.238.38,4594,karen.reto.com,71.43.144.111,443,j73fzlugbhbhy3k8jgmv.com
17-8-2020,13:1:12,172.24.238.38,28631,karen.reto.com,220.218.191.76,443,p7necksgkbynlvmgenv5.org
17-8-2020,13:42:58,172.24.238.38,62511,karen.reto.com,220.218.191.76,80,p7necksgkbynlvmgenv5.org
17-8-2020,13:43:17,172.24.238.38,33644,karen.reto.com,220.218.191.76,80,p7necksgkbynlvmgenv5.org
17-8-2020,13:46:22,172.24.238.38,2099,karen.reto.com,220.218.191.76,80,p7necksgkbynlvmgenv5.org
17-8-2020,13:50:57,172.24.238.38,34901,karen.reto.com,220.218.191.76,80,p7necksgkbynlvmgenv5.org
17-8-2020,13:54:37,172.24.238.38,45702,karen.reto.com,220.218.191.76,80,p7necksgkbynlvmgenv5.org
17-8-2020,13:56:9,172.24.238.38,41899,karen.reto.com,220.218.191.76,80,p7necksgkbynlvmgenv5.org
17-8-2020,13:56:42,172.24.238.38,23936,karen.reto.com,220.218.191.76,80,p7necksgkbynlvmgenv5.org
17-8-2020,14:2:30,172.24.238.38,37324,karen.reto.com,220.218.191.76,80,p7necksgkbynlvmgenv5.org
17-8-2020,14:3:28,172.24.238.38,11778,karen.reto.com,220.218.191.76,80,p7necksgkbynlvmgenv5.org
17-8-2020,14:6:43,172.24.238.38,22897,karen.reto.com,220.218.191.76,80,p7necksgkbynlvmgenv5.org
17-8-2020,14:8:11,172.24.238.38,14924,karen.reto.com,220.218.191.76,80,p7necksgkbynlvmgenv5.org
17-8-2020,14:8:31,172.24.238.38,58307,karen.reto.com,220.218.191.76,80,p7necksgkbynlvmgenv5.org
17-8-2020,14:9:6,172.24.238.38,29897,karen.reto.com,220.218.191.76,80,p7necksgkbynlvmgenv5.org
17-8-2020,14:10:7,172.24.238.38,17658,karen.reto.com,220.218.191.76,80,p7necksgkbynlvmgenv5.org
```

7. *(Extra): En caso de que hayas encontrado que las computadoras del paso 1 y 4 se comunican, determina en qué fecha ocurre la primera comunicación entre estas 2 y qué protocolo se usó.*

La imagen anterior muestra que la fecha en la que ocurre la primera comunicación es el 17-8-2020.

Asimismo, observando los puertos de los récords, es posible notar que se utiliza solo en las primeras dos interacciones el puerto 443 (HTTPS), y a partir de la tercera, el puerto 80 (HTTP). De aquí, se vuelve evidente que se llegó de utilizar un puerto “secure” a uno “no secure”. Recordando que HTTP y HTTPS son protocolos de transferencia de hipertexto entre un usuario y un servidor. Al unir esta información con la obtenida mediante la resolución del presente avance, es posible observar que el usuario de la red interna con IP 172.24.238.38 (karen.reto.com) no solo tiene conexiones sospechosas (dominios anómalos) sino que también intenta entablar conexiones con otras de las computadoras internas de la compañía.

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 partes 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:

- Código para el análisis de la clase ConexionesComputadora mediante diccionarios y hash.
- Pregunta 4.

Andreína Sanánez / A01024927

- Código de solución de las preguntas 1-3.

Ana Paula Katsuda / A01025303

- Código de solución de las preguntas 5-7.