Reflexión Actividad 5.2

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

   e1vrkur1pw73zlhg9asc.ru y ggex1ffe16fwzk3as5vd.net

2. **De 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?**

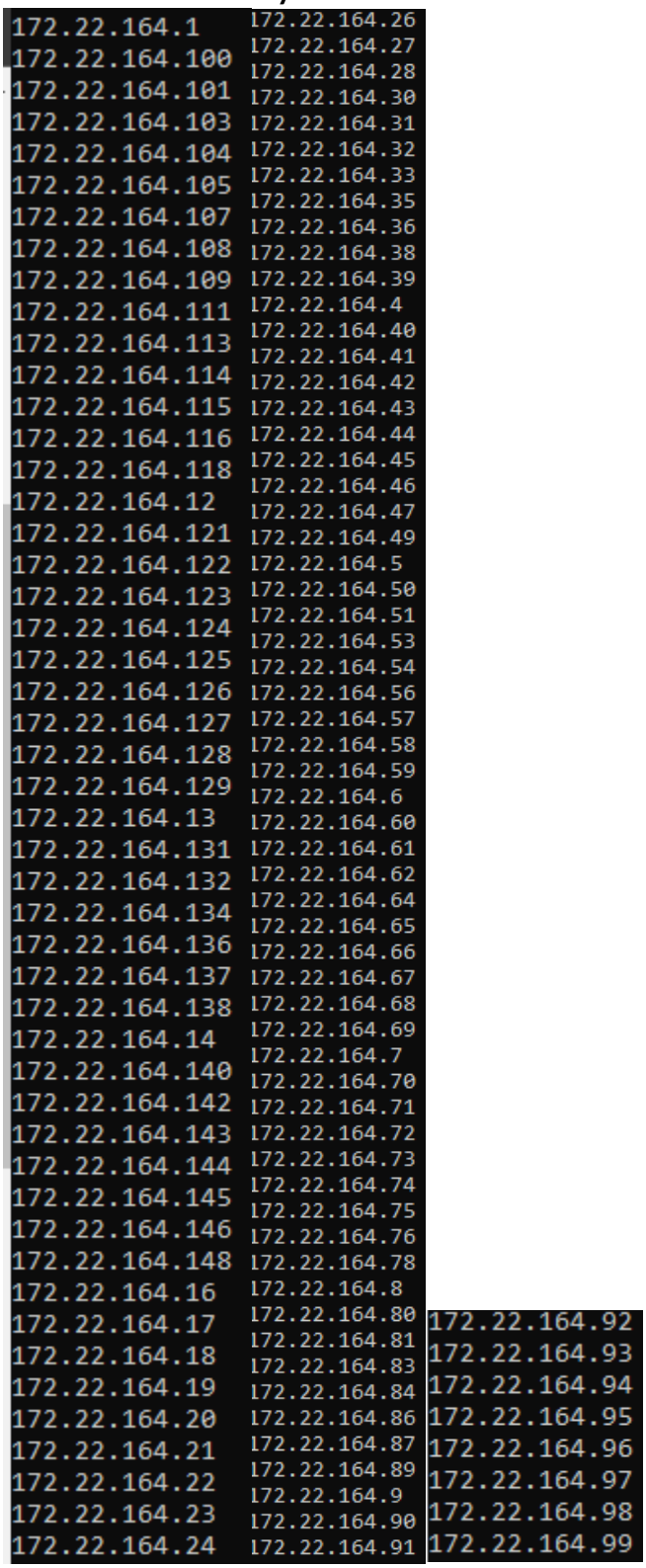
   Nombre: ,e1vrkur1pw73zlhg9asc.ru, IP: 157.0.45.144
   Nombre: ,ggex1ffe16fwzk3as5vd.net, IP: 161.210.17.248

   En caso de que ya se tenga una estructura como un set, que contenga los dominios, junto a el resto de la información del registro, que incluiría su IP, solamente los buscaría, por nombre. Si no se tiene un set, lo crearía para armar una pequeña base de datos para uso posterior.
   Otra alternativa es armar un hash map, que tome como llave los dominios y que contenga como valor el registro completo, para así nada más pasar la llave y que me lleve directamente al registro, de donde se referenciaría a la IP.

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.**

   147

4. **Toma algunas computadoras que no sean server.reto.com o el servidor DHCP. Pueden ser entre 5 y 10. Obtén las IP's únicas de las conexiones entrantes.**



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

   Al ver que pocas computadoras (considerando el tamaño de la base de datos) del dominio reto.com y que solamente las IP únicas para las computadoras que no pertenecen a reto.com son muchas, lo que creo que está sucediendo es que se está evitando utilizar computadoras que estén monitoreadas, al ser parte de reto.com, para llevar a cabo los ataques, pues al las demás no pertenecer al reto.com, asumo que son externas a la propiedad de la escuela y son mejores blancos para formar parte de la botnet.

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

   Ninguna se comunica con alguno de los sitios raros, pues únicamente hay conexiones con los sitios raros desde computadoras de reto.com

7. **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 esta s dos y qué protocolo se usa.**

   Ninguna computadora se conecta con los sitios encontrados en la pregunta 1, por lo que no hay fecha ni protocolo para analizar.

```
Pregunta 7

Ninguna de las IP's encontradas se conecta con alguno de los sitios raros
```

Uso de diccionarios y conjuntos

Para situaciones tales como con la que nos tocó trabajar en este caso, es conveniente tener estructuras como los set, pues al nada más almacenar datos únicos, funcionan como un filtro más simple para cuando se requiere justamente identificar elementos únicos, pues si no se usaran, probablemente programaríamos filtros para corroborar que no se repitan los datos en dentro de la estructura y, por la experiencia que tenemos hasta el momento, lo más probable es que no sean tan eficientes como un set, que forma parte de la STL.

Por el lado de los diccionarios, igualmente son útiles si ya se quiere ubicar los datos en base a un identificador único, pues al conocer el nombre del identificador, nos evitamos el tratar con la búsqueda del elemento, para después extraer su índice, para finalmente realizar las operaciones que se necesiten.