**Reporte Reto 3**

En esta entrega del reto se dio la tarea de ordenar nuestros registros para poder visualizar de mejor manera lo que sucedió dentro de la red “reto.com”. Para lograr esto se nos pidió crear un conjunto en donde estuvieran todos los nombres de los dominios que no pertenecían a la red “reto.com”. Imprimiendo este conjunto me di cuenta de que existían dos nombres lo cuales estaban baste fuera de lo normal. El primero es “in6u9mmzf2o5dwr8o43l.ru” y su IP es “122.210.219.145”, y la segunda es “gncbrmxpm138gzbscrle.ru” y su IP es “178.62.64.51”. Para obtener las IPs de ambas de estas paginas de la manera mas eficiente posible cree un diccionario (Unordered\_Map) en donde la llave representaba la dirección IP y el valor era el nombre de dominio, por lo que itere por todas las llaves checando sus valores hasta encontrar el nombre de ambas paginas e imprimir la llave. Esto tiene una complejidad temporal de O(n). Estoy consciente que es más optimo que los nombres de dominio representaran las llaves y las direcciones IP representaran los valores para así poder obtener las direcciones IP sin tener que iterar y checar los valores de los valores de cada llave. Este método tendría una complejidad temporal de O(1), pero ya que este diccionario se requiere de esta manera en otras partes del programa tiene esta estructura.

Con esta información se hizo un análisis para saber que cuantas de las 31 computadoras que están dentro de nuestra red “reto.com” se han conectado a alguna de estas páginas. Los resultados nos indicaron que 29 de nuestras computadoras se han conectado a la “in6u9mmzf2o5dwr8o43l.ru” solamente mientras que 1 se ha conectado solamente a “gncbrmxpm138gzbscrle.ru”.

Tengo pensado que la única computadora que se conecto a “gncbrmxpm138gzbscrle.ru” fue la causante del ataque ya que es la misma la cual se conecto a todas las otras computadoras de la red. Al igual los puertos que se utilizaron para acceder de esta computadora a las demás son puertos que pertenecen al protocolo TCP el cual permite enviar datos. Es posible que la computadora que se conecto a “gncbrmxpm138gzbscrle.ru” descargo y ejecuto algún código malicioso el cual le permitió mandar más código malicioso a las demás computadoras dentro de la red, el cual realiza la conexión a la otra pagina anómala.