

Emiliano Cabrera - A01025453

Programacion de estructuras de datos y algoritmos fundamentales
29 de noviembre del 2021

Reflexión

Preguntas

```
Hay 358 computadoras

1. ¿Hay algún nombre de dominio que sea anómalo?
   Sí.

2. ¿Cuál es su IP? ¿Cómo determinarías esta información de la manera más eficiente en complejidad temporal?
   La IP es 128.88.113.158
   Con una inspección visual identificamos: http://36ytsfs8ph6iczxioli4.net
   Hicimos una función prototipo de cómo se podrían encontrar dominios anómalos: encontrarAnomalos(datos).
   Para esto usamos como parámetros el largo del dominio y si contiene caracteres no alfanuméricos,
   ya que los dominios largos con una extraña combinación de caracteres alfanuméricos son las características
   más comunes de los dominios anómalos.
   Si se entrenara un modelo de ML para que pudiese reconocer a los dominios anómalos podríamos identificarlos
   Si se entrenara un modelo de ML para que pudiese reconocer a los dominios anómalos podríamos identificarlos
   al momento de que entren o salgan, en una complejidad de O(1).

3. De las computadoras pertenecientes al dominio reto.com determina la cantidad de ips que tienen al menos una conexión entrante.
   91 computadoras de la red interna con al menos una conexion entrante

4. Toma algunas computadoras que no sean server.reto.com o el servidor dhcp. Pueden ser entre 5 y 150. Obtén las ip únicas de las conexiones entrantes.
   -
   192.168.29.1
   192.168.29.10
   192.168.29.100
   192.168.29.101
   192.168.29.102
   192.168.29.103
   192.168.29.104
   192.168.29.105
   192.168.29.106
   192.168.29.107
   192.168.29.108
   192.168.29.11
   192.168.29.110
   192.168.29.111
   192.168.29.112
   192.168.29.113
   192.168.29.114
   192.168.29.115
   192.168.29.116
   192.168.29.117
   192.168.29.118

5. Considerando el resultado de las preguntas 3 y 4, ¿Qué crees que esté ocurriendo en esta red? (Pregunta sin código)
   32 computadoras internas tienen conexiones entrantes. Esto significa que computadoras externas están intentando acceder a la información. De las conexiones entrantes, puede identificarse que existe solo una conexión al dominio anómalo.

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

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 estas 2 y qué protocolo se usó.
   La computadora de Amanda se infectó el: 13/8/2020
   Puerto: 13307
```

1. En efecto, hay nombres anómalos.

2. La IP es 128.88.113.158, se puede entrenar un algoritmo de ML que reconozca dominios anómalos y a su vez obtenga su dirección IP con una complejidad temporal de $O(1)$.

3. Hay 91 computadoras de la red interna con al menos 1 conexión entrante.

4. IPs:

192.168.29.1	192.168.29.104	192.168.29.111
192.168.29.10	192.168.29.105	192.168.29.112
192.168.29.100	192.168.29.106	192.168.29.113
192.168.29.101	192.168.29.107	192.168.29.114
192.168.29.102	192.168.29.108	192.168.29.115
192.168.29.103	192.168.29.11	192.168.29.116
	192.168.29.110	

192.168.29.117	192.168.29.20	192.168.29.6
192.168.29.118	192.168.29.21	192.168.29.60
192.168.29.119	192.168.29.22	192.168.29.62
192.168.29.12	192.168.29.23	192.168.29.63
192.168.29.120	192.168.29.24	192.168.29.64
192.168.29.121	192.168.29.25	192.168.29.65
192.168.29.123	192.168.29.26	192.168.29.66
192.168.29.124	192.168.29.27	192.168.29.67
192.168.29.125	192.168.29.28	192.168.29.68
192.168.29.126	192.168.29.29	192.168.29.69
192.168.29.127	192.168.29.3	192.168.29.7
192.168.29.128	192.168.29.30	192.168.29.70
192.168.29.129	192.168.29.31	192.168.29.71
192.168.29.130	192.168.29.32	192.168.29.72
192.168.29.131	192.168.29.35	192.168.29.73
192.168.29.132	192.168.29.36	192.168.29.74
192.168.29.133	192.168.29.37	192.168.29.75
192.168.29.134	192.168.29.38	192.168.29.76
192.168.29.135	192.168.29.39	192.168.29.77
192.168.29.136	192.168.29.4	192.168.29.78
192.168.29.137	192.168.29.41	192.168.29.79
192.168.29.138	192.168.29.43	192.168.29.8
192.168.29.139	192.168.29.44	192.168.29.81
192.168.29.14	192.168.29.45	192.168.29.82
192.168.29.140	192.168.29.46	192.168.29.83
192.168.29.141	192.168.29.47	192.168.29.84
192.168.29.142	192.168.29.48	192.168.29.85
192.168.29.143	192.168.29.49	192.168.29.87
192.168.29.144	192.168.29.5	192.168.29.89
192.168.29.145	192.168.29.50	192.168.29.9
192.168.29.146	192.168.29.51	192.168.29.91
192.168.29.147	192.168.29.52	192.168.29.92
192.168.29.148	192.168.29.54	192.168.29.93
192.168.29.149	192.168.29.55	192.168.29.94
192.168.29.15	192.168.29.56	192.168.29.95
192.168.29.150	192.168.29.57	192.168.29.96
192.168.29.17	192.168.29.58	192.168.29.97
192.168.29.18	192.168.29.59	192.168.29.98
192.168.29.2		192.168.29.99

5. Hay 91 computadoras con conexiones entrantes, lo cual indica que hay computadoras externas que intentan acceder a su información.
6. La computadora con el dominio amanda.reto.com tuvo una instancia de contacto.
7. La computadora amanda.reto.com hizo contacto con el dominio anómalo el 13/8/2020 mediante el puerto 13307, es decir, se utilizó el protocolo TCP y UDP.

Uso de diccionarios y conjuntos

Los conjuntos permiten analizar grupos de información de manera que se puedan observar todos los distintos valores que contienen, y en el caso de análisis de redes ayudan a generar un listado de direcciones IP únicas o dominios distintos con las que se hacen conexiones. Sirven mucho mejor en conjunto con otras estructuras, algoritmos u otros conjuntos que permitan relacionar el comportamiento entre los dominios pertinentes por frecuencia de comunicación, volumen de tráfico o incluso para determinar anomalías.

Los diccionarios complementan este propósito de una manera excelente. El análisis de redes se ve facilitado por su naturaleza de relacionar llaves y valores, y al combinarlo con los conjuntos puede uno obtener una descripción completa del comportamiento de las computadoras dentro de una red.

En el caso de usar tablas hash capaces de manejar el desbordamiento lineal como la estructura central del diccionario, puede uno obtener cualquier pedazo de información necesaria en un tiempo lineal. La eficiencia depende mucho de la estructura que se use, pero el uso del diccionario reduce los recursos que se le destinan a las búsquedas subsecuentes.

Como toda estructura de almacenamiento, hay desventajas. No se puede visualizar de manera apropiada la información ya que son únicamente valores adjuntados a una llave, apropiado para una estructura denominada diccionario que tiene un concepto (llave) y su descripción (valor o valores). La visualización tomaría una estructura intermediaria que se debería de llenar utilizando ciertos filtros, por lo que un diccionario no ayuda.

Referencias

TCP/UDP Port Finder. adminsub.net. (s.f.). Recuperado de
<https://www.adminsub.net/tcp-udp-port-finder/13307>.