Lourdes Badillo, A01024232

Eduardo Villalpando, A01023646

Programación de Estructuras de Datos y Algoritmos Fundamentales

Profesor Leonardo Chang

Reflexión

I. Preguntas

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

Sí.

De los nombres de dominio encontrados en el paso anterior:

¿Cuál es su ip?

La IP es 161.32.130.251

¿Cómo determinarías esta información de la manera más eficiente en complejidad temporal?

Con una inspección visual identificamos: ds19smmrn47jp3osf6x4.com

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

Una implementación eficiente podría ser tener un algoritmo de machine learning, que vaya aprendiendo qué dominios son anómalos y los detecte en una complejidad O(1)

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.

Hay 32 computadoras pertenecientes al dominio reto.com

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.

Las IP son:

-

172.26.89.105

172.26.89.113

172.26.89.118

172.26.89.123

172.26.89.13
172.26.89.137
172.26.89.139
172.26.89.146
172.26.89.147
172.26.89.149
172.26.89.16
172.26.89.19
172.26.89.26
172.26.89.32
172.26.89.33
172.26.89.35
172.26.89.36
172.26.89.41
172.26.89.54
172.26.89.56
172.26.89.62
172.26.89.67
172.26.89.70
172.26.89.74
172.26.89.75
172.26.89.78
172.26.89.8
172.26.89.82
172.26.89.9
172.26.89.90
172.26.89.93
172.26.89.95

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.

jennifer.reto.com se conectó 3220 al dominio anteriormente mencionado.

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

Si.

(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.

Fecha: 17 de agosto del 2020

Puerto: 965

II. Aportaciones

Para poder realizar este entregable, nos dividimos las diferentes tareas de la siguiente forma:

Tarea	**Responsable**
Crear conjunto de strings para dominios externos	Lourdes
Crear diccionario <string, ConexionesComputadora> para todas las IP's de los datos	Eduardo
Llenar diccionario de computadoras siempre que no exista la llave dentro de los datos, y posteriormente llenar ConexionesComputadora con los datos correspondientes	Lourdes
Implementar función para detectar si un dominio es anómalo	Eduardo
Implementar función para iterar por todas las computadoras y determinar si alguna es anómala	Lourdes
Filtrar computadoras pertenecientes a reto.com y con numero de conexiones superior a uno	Eduardo
Iterar por todas las computadoras externas a reto.com y almacenar las conexiones entrantes en un set	Lourdes
Implementar función para obtener conexiones de computadora anómala	Eduardo
Implementar función para obtener fecha y puerto de primera conexión entrante de computadora anómala	Lourdes