

Karla Mondragón, A01025108  
Ximena Sánchez, A01275072  
31 de octubre 2021  
Programación de Estructuras de Datos y Algoritmos Fundamentales  
Jorge Rodríguez

### Reporte Reto 3 - Actividad Integral sobre el uso de códigos hash

1. Hay algún nombre de dominio que sea anómalo (Esto puede ser con inspección visual).  
A partir de la inspección visual podemos determinar que los siguientes dominios tienen una nomenclatura anómala.

```
Los domnios anómalos son 2ngv8iamw6s87eo4z6c7.org y 4ftjzr4g5u8gawcsnjv1.com
```

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?

```
La dirección IP de 2ngv8iamw6s87eo4z6c7.org es: 88.10.73.146  
La dirección IP de 4ftjzr4g5u8gawcsnjv1.com es: 42.153.2.226
```

Lo determinamos de la manera más óptima en complejidad temporal al agregar el atributo domain a ConexionesComputadora para hacerlo de forma más eficiente

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.

```
=====
CANTIDAD DE IPs CON AL MENOS UNA CONEXION ENTRANTE =====
No. de equipos con al menos una conexión entrante del dominio reto.com: 27
=====
```

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

```
Conexiones entrantes de jack.reto.com:
172.22.55.15
Conexiones entrantes de mary.reto.com:
172.22.55.124
172.22.55.93
172.22.55.86
172.22.55.27
172.22.55.92
172.22.55.74
172.22.55.94
172.22.55.4
172.22.55.7
172.22.55.110
172.22.55.15
172.22.55.59
172.22.55.116
172.22.55.44
172.22.55.1
172.22.55.145
172.22.55.123
172.22.55.88
172.22.55.58
172.22.55.113
172.22.55.57
172.22.55.129
172.22.55.105
172.22.55.29
172.22.55.98
172.22.55.19
172.22.55.6
Conexiones entrantes de rebecca.reto.com:
172.22.55.15
```

5. Considerando el resultado de las preguntas 3 y 4, ¿Qué crees que está ocurriendo en esta red? (Pregunta sin código)  
Consideramos que la ip 42.153.2.226 infecto de alguna forma a la computadora de mary.reto.com con ip 172.22.55.1
6. Para las ips encontradas en el paso anterior, determina si se han comunicado con los datos encontrados en la pregunta 1.

```
Conexiones salientes de mary.reto.com:
El equipo de mary.reto.com tuvo 1 conexion saliente a 2ngv8iamw6s87eo4z6c7.org
El equipo de mary.reto.com tuvo 1 conexion saliente a 4ftjzr4g5u8gawcsnjv1.com
```

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.  
Se realiza el 14 de agosto de 2020 (12:00:43 p. m.) utilizando la vulnerabilidad del puerto 443

```
La primera comunicación entre la ip de Mary y 88.10.73.146 fue: 14-8-2020
La primera comunicación entre la ip de Mary y 42.153.2.2262 fue: 14-8-2020
La comunicación entre la ip de Mary y 88.10.73.146 se hizo utilizando la vulnerabilidad del puerto 443 el cual corresponde al protocolo HTTPS.
La comunicación entre la ip de Mary y 42.153.2.2262 hizo utilizando la vulnerabilidad del puerto443 el cual corresponde al protocolo HTTPS.
```

Retomando la información de la primera entrega del reto, se sabe que el puerto 443 es utilizado por HTTPS, Threat y Trojan. El UDP y SCTP son utilizados por HTTPS. Por lo que los protocolo que se usó fue el HTTPS.

**Participaciones:**

1. Cree un conjunto de strings. En este debes agregar los nombres de los dominios/computadoras que no pertenezcan al dominio reto.com. - Ximena
2. Crea un diccionario de pares <string, ConexionesComputadora> usando la clase creada en el reto pasado. Este diccionario debe ser llenado con todas las ips en los datos. Por cada una, es necesario registrar todas las conexiones que hayan salido desde esta ip o hayan sido recibidas por la misma. - Ximena
3. Pregunta 1 - las dos
4. Pregunta 2 - las dos
5. Pregunta 3 - Ximena
6. Pregunta 4 - Karla
7. Pregunta 5 - las dos
8. Pregunta 6 - Ximena
9. Pregunta 7 - Karla