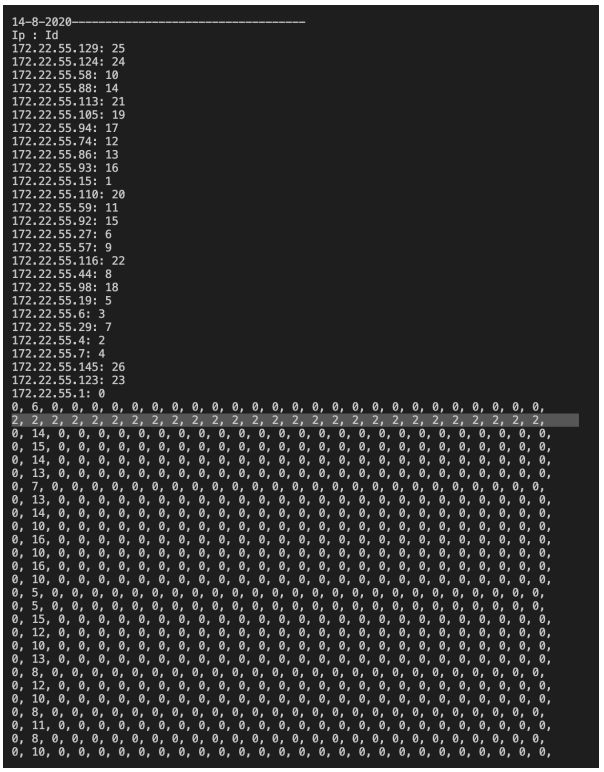
Karla Mondragón, A01025108
Ximena Sánchez, A01275072
30 de noviembre 2021
Programación de Estructuras de Datos y Algoritmos Fundamentales
Jorge Rodríguez

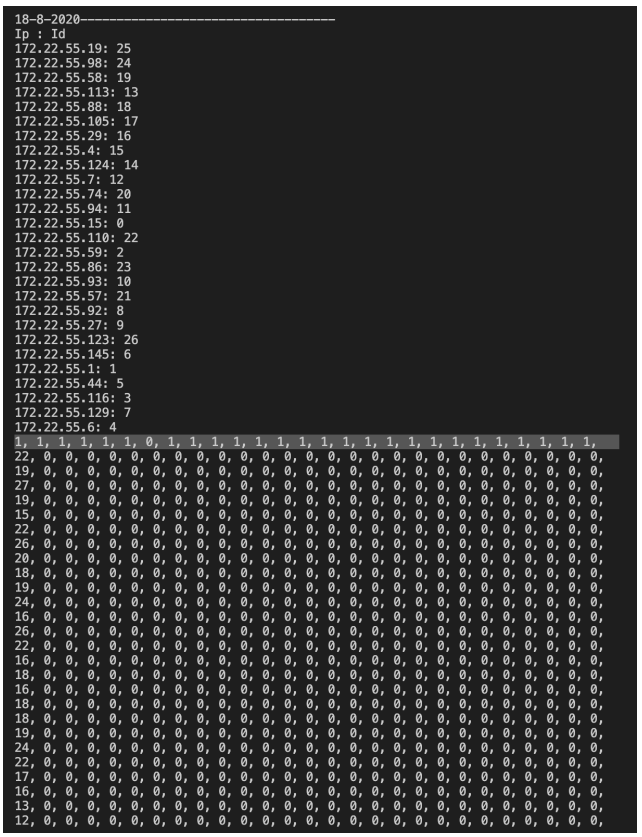
Reto 5 - Actividad Integral de Grafos

1. **Utilizando un grafo con las conexiones entre las ip de la red interna, determina la cantidad de computadoras con las que se ha conectado A por día. ¿Es el vértice que más conexiones salientes hacia la red interna tiene?**

Si, la IP interna A es el equipo de mary.reto.com con ip 172.22.55.15, la cual se comunica con algunas otras computadoras internas del dominio reto.com:

- Los días 14 y 18 de agosto esta ip, se conectó con las siguientes computadoras.

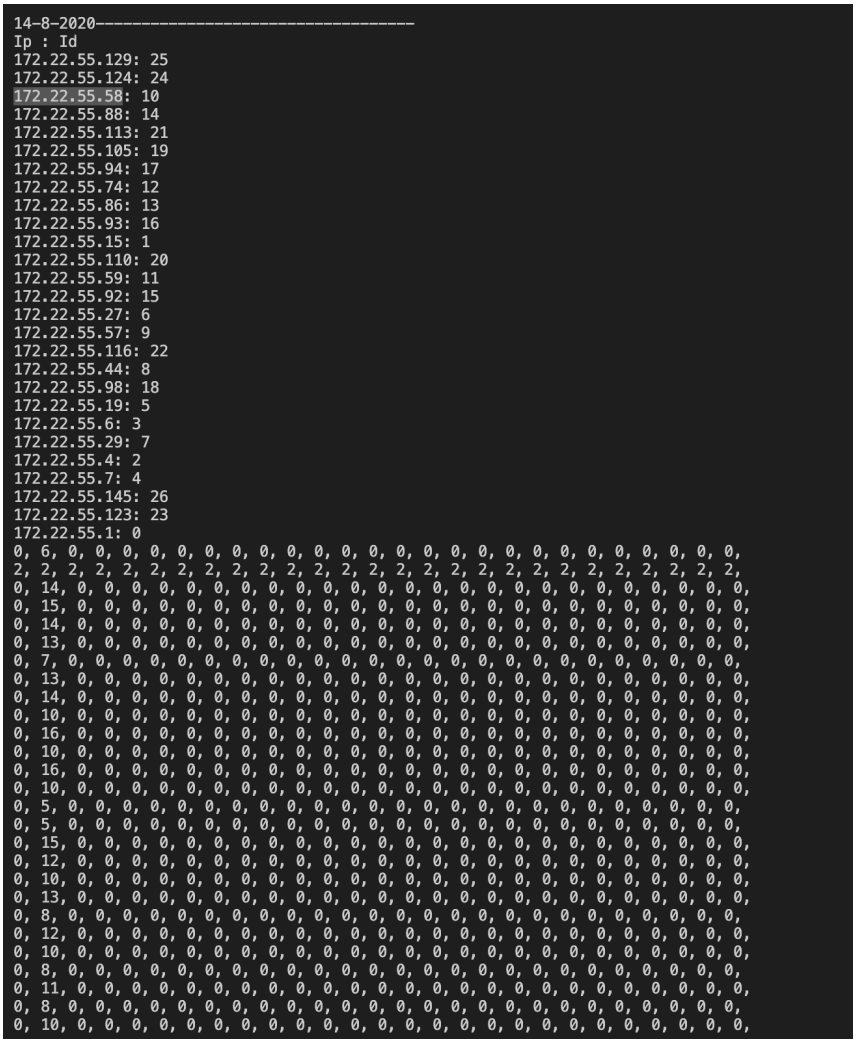




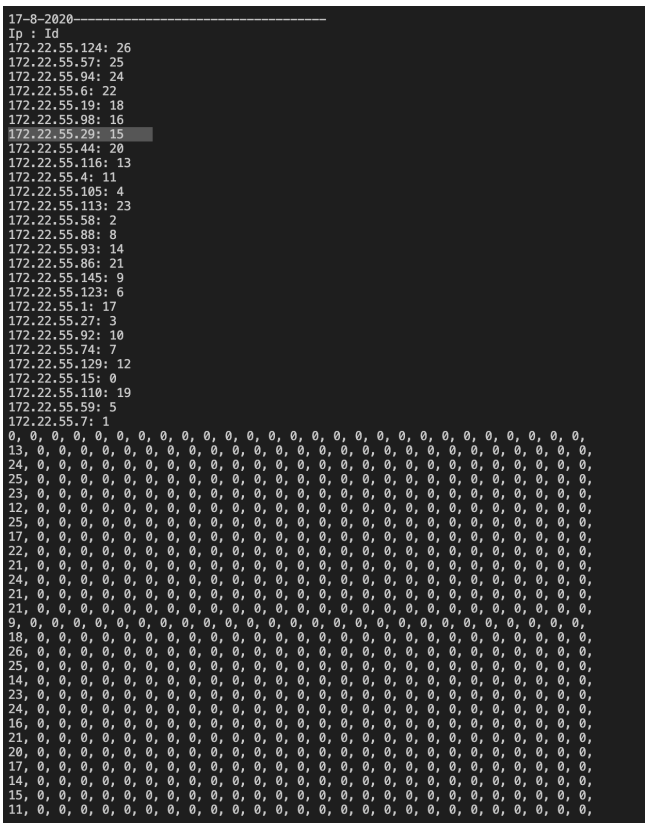
2. **Utilizando el grafo del punto anterior, ubica la cantidad de computadoras que se han conectado hacía A por día. ¿Existen conexiones de las demás computadoras hacía A?**

Si, la IP interna A es el equipo de mary.reto.com con ip 172.22.55.15 , hacia la cual se comunican algunas otras computadoras internas del dominio reto.com:

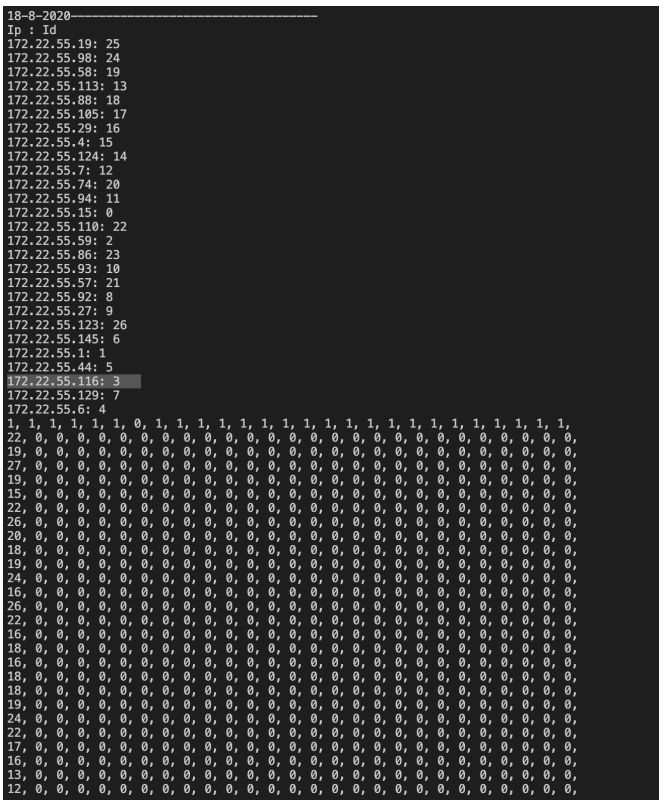
- El 14 de agosto del 2020, las ips 172.22.55.58 y 172.22.55.74, fueron las que más tuvieron conexiones salientes al equipo de mary.reto.com, con un total de 16 conexiones.



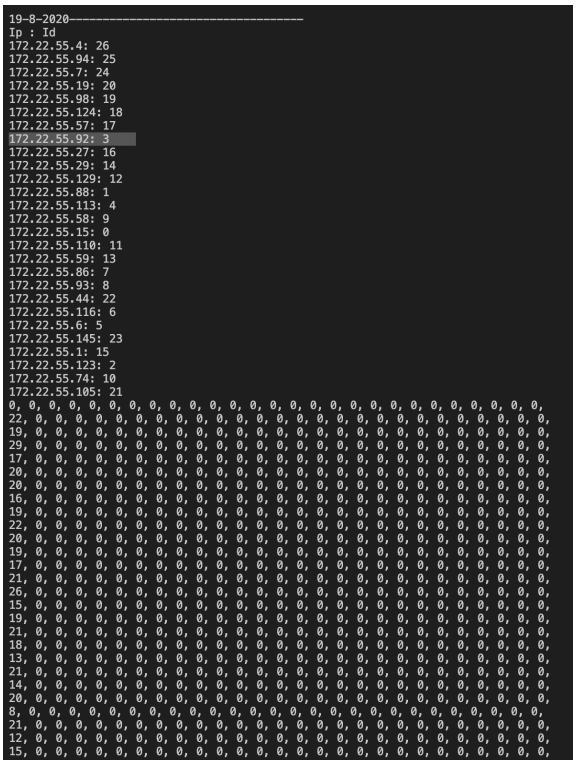
- El 17 de agosto del 2020, la ip 172.22.55.29 tuvo un total de 26 conexiones salientes hacia el equipo mary.reto.com.



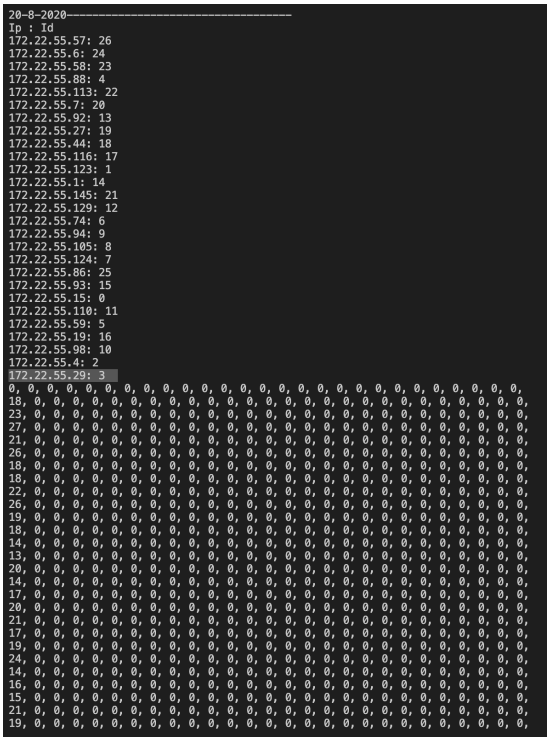
- El 18 de agosto se puede observar que la ip con mayores conexiones salienteshacia el equipo mary.reto.com fue la ip 172.22.55.116 con 27 conexiones.



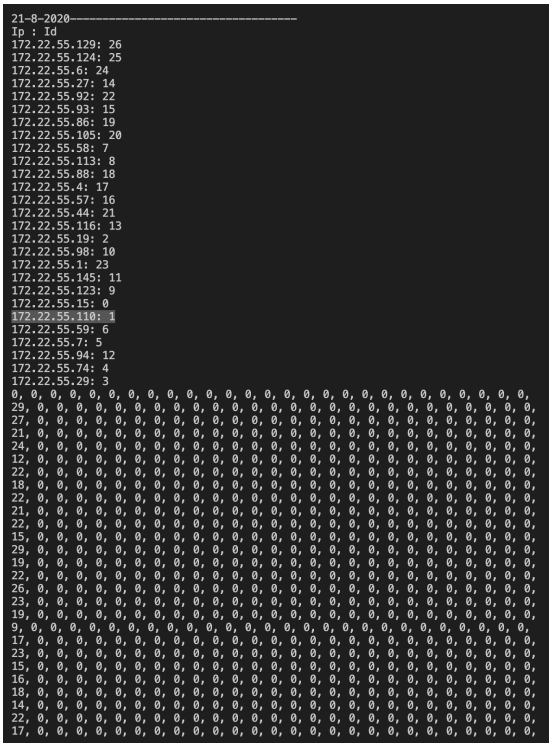
- El día 19 de agosto, la ip 172.22.55.92 tuvo 29 conexiones salientes al equipo de mary.reto.com



- Se puede observar que el 20 de agosto, la ip 172.22.55.29 tuvo la mayor cantidad de conexiones salientes, con un total de 27.



- Y por último, el 21 de agosto, la ip con mayor conexiones salientes al equipo de mary.reto.com fue la 172.22.55.110 con 29 conexiones.



```
21-8-2020----------------------------------
Ip : Id
172.22.55.129: 26
172.22.55.124: 25
172.22.55.6: 24
172.22.55.27: 14
172.22.55.92: 22
172.22.55.93: 15
172.22.55.86: 19
172.22.55.105: 20
172.22.55.58: 7
172.22.55.113: 8
172.22.55.88: 18
172.22.55.4: 17
172.22.55.57: 16
172.22.55.44: 21
172.22.55.116: 13
172.22.55.19: 2
172.22.55.98: 10
172.22.55.1: 23
172.22.55.145: 11
172.22.55.123: 9
172.22.55.15: 0
172.22.55.110: 1
172.22.55.59: 6
172.22.55.7: 5
172.22.55.94: 12
172.22.55.74: 4
172.22.55.29: 3
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
29, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
27, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
21, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
24, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
12, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
22, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
18, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
22, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
21, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
22, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
15, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
29, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
19, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
22, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
26, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
23, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
19, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
9, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
17, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
23, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
15, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
16, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
18, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
14, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
22, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
17, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
```

Pensamos que todas estas conexiones salientes hacia el equipo A, se conectan al equipo solicitando instrucciones.

3. Utilizando un grafo de conexiones a sitios web, determina cuántas computadoras se han conectado a B por día.

Dominio anómalo que denominamos B = 4ftjzr4g5u8gawcsnjv1.com con dirección IP de 42.153.2.226

```
------------------- Computadoras se han conectado a B por día (4ftjzr4g5u8gawcsnjv1.com-- > 42.153.2.226) -------------------
cantidad de conexiones: 0
11-8-2020----------------------------------
Ip : Id

cantidad de conexiones: 0
12-8-2020----------------------------------
Ip : Id

cantidad de conexiones: 0
13-8-2020----------------------------------
Ip : Id

cantidad de conexiones: 154
14-8-2020----------------------------------
Ip : Id
mary.reto.com: 1
4ftjzr4g5u8gawcsnjv1.com: 0
0, 0,
154, 0,

cantidad de conexiones: 236
17-8-2020----------------------------------
Ip : Id
mary.reto.com: 1
4ftjzr4g5u8gawcsnjv1.com: 0
0, 0,
236, 0,
```

```
cantidad de conexiones: 245
18-8-2020-----------------------------------
Ip : Id
mary.reto.com: 1
4ftjzr4g5u8gawcsnjv1.com: 0
0, 0,
245, 0,

cantidad de conexiones: 281
19-8-2020-----------------------------------
Ip : Id
mary.reto.com: 1
4ftjzr4g5u8gawcsnjv1.com: 0
0, 0,
281, 0,

cantidad de conexiones: 238
20-8-2020-----------------------------------
Ip : Id
mary.reto.com: 1
4ftjzr4g5u8gawcsnjv1.com: 0
0, 0,
238, 0,

cantidad de conexiones: 217
21-8-2020-----------------------------------
Ip : Id
mary.reto.com: 1
4ftjzr4g5u8gawcsnjv1.com: 0
0, 0,
217, 0,
```

Como se puede observar, B solamente interacciona con A y comienza el 14 de agosto del 2020. Después de esta primera interacción (que es la que tiene menor cantidad de conexiones), A y B interactúan todos los días, A siempre conectándose a B y nunca viceversa. El día 18 es cuando mary.reto.com se conecta más veces a B con 281 conexiones.

4. **Utilizando el mismo grafo del punto anterior, indica cuántas computadoras se han conectado a C por día**.

Un sitio web normal que tiene un volumen de tráfico anómalo un día, el que denominamos C es reddit.com.

```
------------------- Computadoras se han conectado a C por día (reddit.com) -------------------
cantidad de conexiones: 7
11-8-2020-----------------------------------
Ip : Id
patrick.reto.com: 3
jack.reto.com: 5
justin.reto.com: 2
emily.reto.com: 4
reddit.com: 0
jennifer.reto.com: 1
0, 0, 0, 0, 0, 0,
2, 0, 0, 0, 0, 0,
1, 0, 0, 0, 0, 0,
1, 0, 0, 0, 0, 0,
2, 0, 0, 0, 0, 0,
1, 0, 0, 0, 0, 0,

cantidad de conexiones: 11
12-8-2020-----------------------------------
Ip : Id
anna.reto.com: 9
jack.reto.com: 8
patricia.reto.com: 7
mark.reto.com: 6
samantha.reto.com: 1
michelle.reto.com: 3
melissa.reto.com: 5
reddit.com: 0
jennifer.reto.com: 2
catherine.reto.com: 4
0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
1, 0, 0, 0, 0, 0, 0, 0, 0, 0,
1, 0, 0, 0, 0, 0, 0, 0, 0, 0,
1, 0, 0, 0, 0, 0, 0, 0, 0, 0,
2, 0, 0, 0, 0, 0, 0, 0, 0, 0,
2, 0, 0, 0, 0, 0, 0, 0, 0, 0,
1, 0, 0, 0, 0, 0, 0, 0, 0, 0,
1, 0, 0, 0, 0, 0, 0, 0, 0, 0,
1, 0, 0, 0, 0, 0, 0, 0, 0, 0,
1, 0, 0, 0, 0, 0, 0, 0, 0, 0,
```

```
cantidad de conexiones: 364
18-8-2020-----------------------------------
Ip : Id
kevin.reto.com: 27
anna.reto.com: 25
jack.reto.com: 22
eric.reto.com: 21
matthew.reto.com: 19
jennifer.reto.com: 4
reddit.com: 0
rebecca.reto.com: 23
gregory.reto.com: 18
ryan.reto.com: 12
john.reto.com: 13
sarah.reto.com: 17
catherine.reto.com: 5
mary.reto.com: 16
emily.reto.com: 7
michelle.reto.com: 24
christine.reto.com: 3
katherine.reto.com: 20
justin.reto.com: 2
jessica.reto.com: 1
charles.reto.com: 6
patricia.reto.com: 8
samantha.reto.com: 26
patrick.reto.com: 9
melissa.reto.com: 11
ashley.reto.com: 10
larry.reto.com: 14
mark.reto.com: 15
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
19, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
16, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
12, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
11, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
9, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
15, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
13, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
15, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
14, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
12, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
11, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
16, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
13, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
10, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
19, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
29, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
17, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
14, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
12, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
12, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
```

```
cantidad de conexiones: 4
19-8-2020-----------------------------------
Ip : Id
eric.reto.com: 4
justin.reto.com: 3
jennifer.reto.com: 2
reddit.com: 0
mark.reto.com: 1
0, 0, 0, 0, 0,
1, 0, 0, 0, 0,
1, 0, 0, 0, 0,
1, 0, 0, 0, 0,
1, 0, 0, 0, 0,

cantidad de conexiones: 13
20-8-2020-----------------------------------
Ip : Id
patrick.reto.com: 7
larry.reto.com: 6
justin.reto.com: 1
jennifer.reto.com: 9
john.reto.com: 8
reddit.com: 0
emily.reto.com: 3
rebecca.reto.com: 5
jessica.reto.com: 2
katherine.reto.com: 4
0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
1, 0, 0, 0, 0, 0, 0, 0, 0, 0,
3, 0, 0, 0, 0, 0, 0, 0, 0, 0,
1, 0, 0, 0, 0, 0, 0, 0, 0, 0,
3, 0, 0, 0, 0, 0, 0, 0, 0, 0,
1, 0, 0, 0, 0, 0, 0, 0, 0, 0,
1, 0, 0, 0, 0, 0, 0, 0, 0, 0,
1, 0, 0, 0, 0, 0, 0, 0, 0, 0,
1, 0, 0, 0, 0, 0, 0, 0, 0, 0,
1, 0, 0, 0, 0, 0, 0, 0, 0, 0,

cantidad de conexiones: 14
21-8-2020-----------------------------------
Ip : Id
sarah.reto.com: 9
justin.reto.com: 6
rebecca.reto.com: 8
jack.reto.com: 7
charles.reto.com: 1
michelle.reto.com: 10
larry.reto.com: 5
reddit.com: 0
emily.reto.com: 4
patricia.reto.com: 2
anna.reto.com: 3
```

El sitio de Reddit tenía un tráfico bajo que no pasaba de las 15 conexiones antes del 17 de agosto del 2020 hasta que el día 18 alcanza las 364 conexiones. Se observa que la dirección IP A solamente se conecta a C el 18, previamente no se había conectado y en días posteriores no se vuelve a conectar.

5. **(Pregunta sin código): Investiga que es un ping sweep, un DDoS, un servidor de comando y control y un botmaster. ¿Ves estos elementos en tus datos?**

   a. **Ping Sweep**

Técnica de escaneo de red utilizada para determinar cuál de un rango de direcciones IP se asigna a host activos (computadoras) (TechTarget, s.f). Consiste en solicitudes de eco ICMP (Internet Control Message Protocol) enviadas a múltiples hosts y si la dirección determinada está activa devuelve una respuesta de eco ICMP. Requiere de una dirección IP o el nombre del dominio del sitio web (TechTarget, s.f).

Creemos que una vez que el equipo mary.reto.com fue infectado, se utilizó esta técnica para explorar los equipos activos en el dominio y poder duplicar el malware.

   b. **DDoS**

Un DDoS o Distributed Denial of Service es un delito cibernético en el que el atacante inunda un servidor con tráfico de internet para evitar que lxs usuarixs accedan a sitios o servicios en línea (Fortinet, s.f). // lo que pasó con reddit ahorita redactó.

Una vez que los equipos infectados del dominio reto.com, entraron en un modo de espera, se activan el 18 de agosto generando un ataque DDoS al sitio C, reddit.com, ya que de pronto presenta un tráfico mucho mayor (casi 25 veces mayor) al usual, lo que nos lleva a pensar que las computadoras de reto.com (por instrucciones de un código malicioso) intentaron inundar al servidor de C. Una vez que este tráfico se presenta, la cantidad de conexiones hacía este sitio vuelven a la normalidad (no supera las 15 conexiones ningún otro día).

   c. **Servidor de comando y de control**

También llamado C&C, es un método que se utiliza para distribuir y controlar el malware. Este método funciona a través de un servidor central que distribuye de manera anónima malware a otras computadoras. Es un método engañoso pues una computadora infectada puede destruir toda una red completa. Una vez que el malware se ejecuta en una computadora, el servidor de comando y control puede ordenarle que se duplique y que se propague fácilmente.

El 14 de agosto a las 12:00:43 hrs, el equipo mary.reto.com se comunica con el servidor 4ftjzr4g5u8gawcsnjv1.com con dirección IP de 42.153.2.226, quien le envía las órdenes de duplicar el malware en toda la red interna en espera de la activación del DDoS.

   d. **Botmaster**

Un botmaster es una persona o equipo que opera el comando y control de botnets. Desde una ubicación remota proporciona dirección a las computadoras comprometidas en el botnet. Una botnet es una colección de computadoras comprometidas por código malicioso

y controladas a través de una red, estas redes a menudo se instalan en máquinas comprometidas a través de varias formas de instalación remota de código. El botmaster por lo general ocultará su identidad a través de herramientas que ocultan su dirección de IP. Los bots están configurados para autenticar la estación de comando y control mediante contraseñas o claves para permitir el control remoto.

El 14 de agosto a las 12:00:29 hrs el equipo de mary.reto.com se comunica por primera y única ocasión con el dominio 2ngv8iamw6s87eo4z6c7.org, quien creemos puede ser el equipo botmaster ya que después de infectar al equipo de mary.reto.com esta comienza a comunicarse con el Servidor de Comando y Control en espera de instrucciones.

Participaciones:

- ***Código***
  - **Pregunta 1** - Karla
  - **Pregunta 2** - Karla
  - **Pregunta 3 -** Ximena
  - **Pregunta 4 -** Ximena
- ***Documento***
  - **Pregunta 1** - Ximena
  - **Pregunta 2** - Ximena
  - **Pregunta 3** - Karla
  - **Pregunta 4 -** Karla
  - **Pregunta 5**
    - **A -** Karla
    - **B -** Karla
    - **C** - Ximena
    - **D** - Ximena

Referencias

Bogna John. (2021). *What Is a "Command and Control Server" for Malware?* [Sitio Web]. Recuperado de: https://www.howtogeek.com/726136/what-is-a-command-and-control-server-for-malware/

Fortinet. (S.f). DDoS Meaning: What is DDoS? [Sitio Web]. Recuperado de https://www.fortinet.com/resources/cyberglossary/ddos-attack

TechTarget. (S.f). Ping Sweep (ICMP Sweep). [Sitio Web]. Recuperado de https://www.techtarget.com/searchnetworking/definition/ping-sweep-ICMP-sweep

Radware.(s.f). Botmaster. [Sitio Web].Recuperado de: https://www.radware.com/security/ddos-knowledge-center/ddospedia/botmaster/

Mezquita,T.(2019).Bot, Botnet, Bot Herder, and Bot Master. [Sitio Web]. Recuperado de: https://cyberhoot.com/cybrary/bot-botnet-bot-herder-and-bot-master/#:~:text=A%20Bot%20Master%20is%20the,compromised%20computers%20in%20the%20botnet.