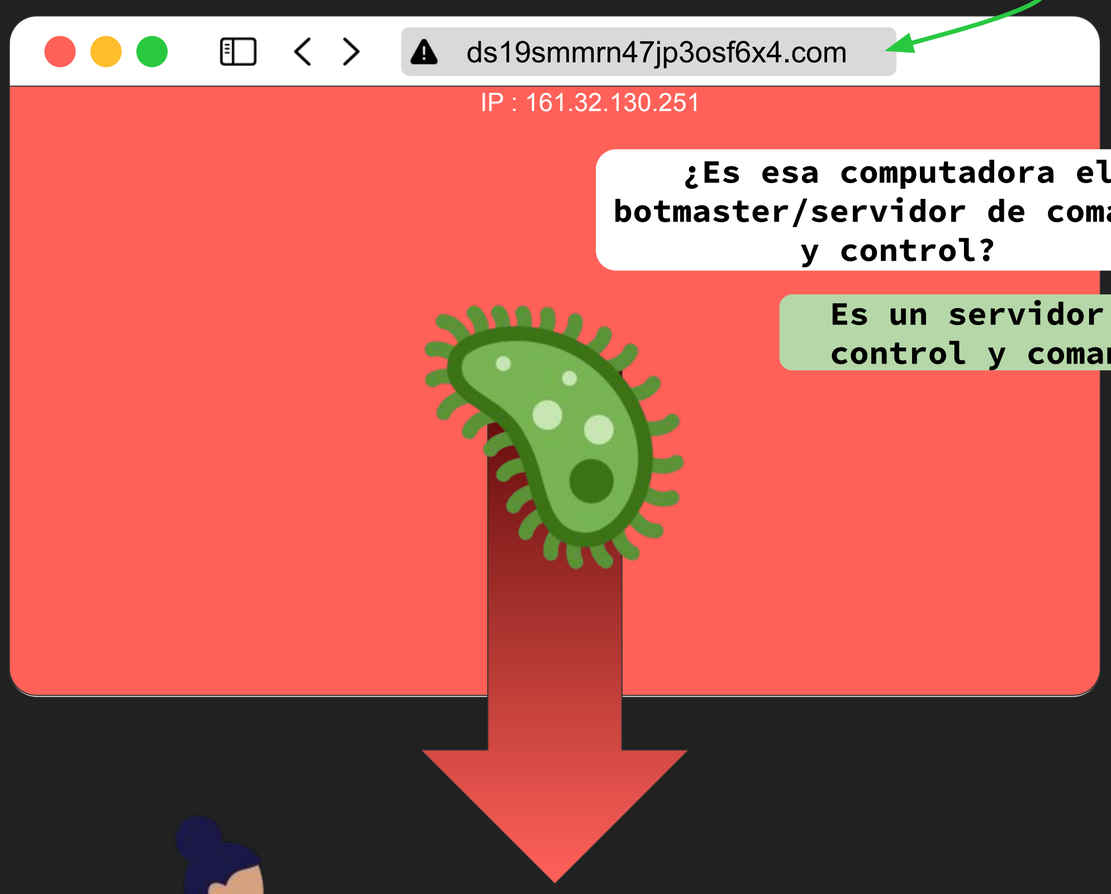
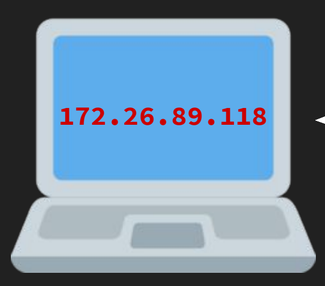
$ cd “Evidencia Final”

¿Qué sitio es el usado para descargar la infección y sirve para controlar las computadoras?



¿Es esa computadora el botmaster/servidor de comando y control?

Es un servidor de control y comando

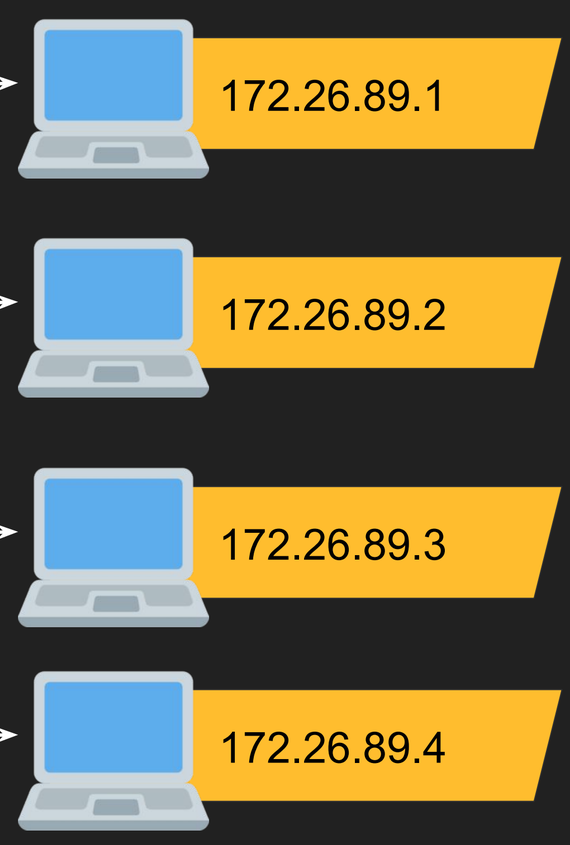


Jennifer
IP: 172.26.89.118

¿Qué computadora es la primera afectada?

¿Qué se hace y cuándo para distribuir la infección a las otras computadoras de la red interna?

El 17/8/2020 la computadora de Jennifer se conecta a 287 computadoras de la red interna. A esto se le llama **ping sweep**.



¿Las computadoras infectadas se conectan a la infectada inicial, al sitio web, o esperan instrucciones?

Las computadoras infectadas se comunican con la infectada inicial

¿Qué ataque se hace y hacia qué sitio?

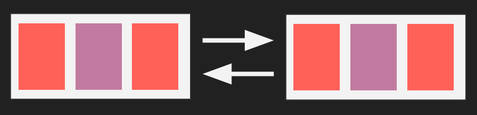
Las respuestas de todas las computadoras forman un ataque DDoS a la computadora infectada

¿Qué estructura de datos te fue menos útil para determinar la información del ataque?

Array/Vector — Entrega 1

✔ Muestra de forma cronológica las conexiones
❌ No permite agruparlas por origen/destino

Linked List — Entrega 2

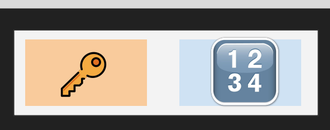


✔ Permite tener una cantidad dinámica de elementos fácilmente modificable. En una lista doblemente enlazada se puede usar el método LIFO y FIFO
❌ Para acceder a un elemento, es necesario recorrer el resto

Set — Entrega 3

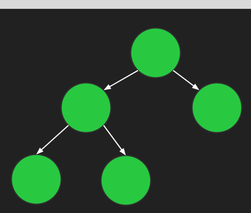
✔ Nos permitió identificar las computadoras, sin repetirlas
❌ No sabíamos las conexiones entrantes y salientes de cada una

Map — Entrega 3



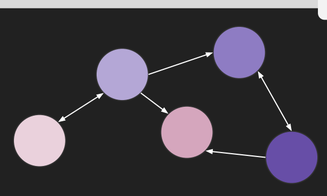
✔ Permite asignar a los valores un identificador
❌ No muestra las conexiones entre los nodos

Binary Search Tree — Entrega 4



✔ Los datos se podían ordenar al insertarlos
❌ No sabíamos todas las conexiones entre los nodos

Graph — Entrega 5



✔ Nos permitió definir la dirección de las conexiones, usando los mismos nodos
Pudimos determinar la cantidad de conexiones entrantes y salientes de cada computadora, para cada día
❌ Fue la más difícil de implementar

¿Qué estructura de datos te fue más útil para determinar la información del ataque?

¿Qué harías diferente o cómo podrías mejorar tu detección de ataques en una red usando lo aprendido en el curso?

Detectar dominios anómalos o no frecuentemente visitados y llevar registro de actividad inusual

$ whoami
Eduardo Villalpando, A01023646
Lourdes Badillo, A01024232