Programación de Estructura de datos y algoritmos

Reflexión Actividad 5.2

Alumno:

Luis Eduardo Aguirre A01749322

Francisco Urquizo Schnaas A01028786

Profesor:

Vicente Cubells

Fecha de entrega:

21 de Noviembre del 2023

Preguntas:

1. **Hay algún nombre de dominio en el conjunto que sea anómalo (Esto puede ser con inspección visual).**
   Sitio raro 1: 86boe9v31ro4yi83dxsj.com
   Sitio raro 2: 7rszfis6fls3zzwhnvm8.net

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?**
   IP sitio raro 1: 28.104.166.194
   IP sitio raro 2: 19.99.251.70

   Para determinar las direcciones IPs de ambos sitios raros, se optó por modificar la primera estructura requerida en esta entrega. En vez de hacer un conjunto de los nombres de las computadoras que no pertenecieran a reto.com, se hizo un mapa cuya llave sería el nombre de la computadora y cuyo valor sería la dirección IP de dicho nombre. De esta forma, las IPs de los sitios raros pudieron ser determinadas en **tiempo constante**.

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.**
   Computadoras pertenecientes al dominio reto.com con al menos una conexión entrante: 253

4. **Toma algunas computadoras que no sean server.reto.com o el servidor DHCP. Pueden ser entre 5 y 10. Obtén las IPs únicas de las conexiones entrantes.**
   IPs de 5 computadoras que no son server.reto.com y no pertenecen al servidor DHCP:
   192.168.86.1
   192.168.86.2
   192.168.86.3
   192.168.86.4
   192.168.86.5

   Se adiciona al vector la IP que se sabe que tiene una conexión con los sitios raros para demostrar la funcionalidad del código:
   192.168.86.1
   192.168.86.2
   192.168.86.3
   192.168.86.4
   192.168.86.5
   192.168.86.22

Cantidad de IPs únicas entrantes: 1
IPs únicas de conexiones entrantes:
192.168.86.22

5. **Considerando el resultado de las preguntas 3 y 4, ¿Qué crees que esté ocurriendo en esta red? (Pregunta sin código)**
   La pregunta 3 indica que la enorme mayoría de las computadoras pertenecientes al dominio reto.com (las computadoras de la red interna) tienen al menos una conexión entrante. La pregunta 4 demuestra que 6 de las computadoras de la red tienen una sola IP que establece una conexión con ellas, la cual es “192.168.86.22”. Esto puede indicar que la computadora con la IP antes mencionada muy probablemente fue la responsable de propagar la infección de la botnet por el servidor interno.

6. **Para las IPs encontradas en el paso anterior, determina si se han comunicado con los datos encontrados en la pregunta 1.**
   Conexiones entre IPs únicas y sitio raro 86boe9v31ro4yi83dxsj.com:

   Conexiones entre IPs únicas y sitio raro 7rszfis6fls3zzwhnvm8.net:

   El código indica que las conexiones entre las IPs únicas y ambos sitios raros son inexistentes. Es decir, no hubieron conexiones entre las IPs en cuestión y los datos encontrados en la pregunta 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 dos y qué protocolo se usa.**
   No hubo una conexión entre una de las 5 IPs y el sitio 86boe9v31ro4yi83dxsj.com

   No hubo una conexión entre una de las 5 IPs y el sitio 7rszfis6fls3zzwhnvm8.net

   Por el hecho de que el código generado para la contestación de la pregunta anterior indicó que no existen conexiones de la naturaleza estipulada, no se puede determinar una fecha de conexión ni el protocolo empleado.

Investigación y reflexión de la importancia y eficiencia del uso de los diccionarios y conjuntos

Luis Eduardo:

Los diccionarios en programación, también conocidos como mapas o hash maps, son estructuras de datos esenciales para almacenar y acceder rápidamente a información. Su importancia en la detección de accesos maliciosos, especialmente en la gestión de redes de bots, es considerable.

Un diccionario permite almacenar pares de datos, como una clave y su valor correspondiente. En el contexto de la seguridad informática, estas claves pueden ser direcciones IP, identificadores de usuarios, o patrones de comportamiento, mientras que los valores asociados pueden incluir detalles como la frecuencia de acceso, la naturaleza de las solicitudes, o marcas de tiempo.

La eficiencia de los diccionarios radica en su capacidad para realizar búsquedas rápidas. En la detección de accesos maliciosos, esto es crucial. Por ejemplo, si un sistema detecta un acceso sospechoso, puede consultar rápidamente el diccionario para verificar si la dirección IP correspondiente ha sido identificada previamente como maliciosa. Esto permite una respuesta rápida y eficiente, reduciendo el riesgo de daño.

Además, los diccionarios facilitan la identificación de patrones. En una red de bots, ciertos patrones de comportamiento, como el acceso simultáneo desde múltiples ubicaciones, pueden ser indicativos de una actividad maliciosa. Al almacenar y analizar estos patrones utilizando diccionarios, los sistemas de seguridad pueden detectar y responder a estas amenazas de manera más efectiva.

En resumen, los diccionarios son herramientas poderosas contra los accesos maliciosos a través de redes de bots. Su habilidad para almacenar grandes cantidades de datos y realizar búsquedas rápidas los convierte en un componente esencial en la detección y prevención de ataques cibernéticos.

Francisco Urquizo:

Los conjuntos, o sets, son otra estructura de datos fundamental en la programación, particularmente útiles en la detección de accesos maliciosos. A diferencia de los diccionarios, los conjuntos se centran en almacenar elementos únicos, lo que los hace ideales para identificar y manejar intentos de acceso repetidos o anormales.

En el contexto de una red de bots, los conjuntos pueden ser utilizados para rastrear direcciones IP o identificadores únicos. Si un sistema detecta múltiples intentos de acceso desde la misma fuente, esto puede ser un indicativo de un comportamiento de bot. Los conjuntos permiten registrar estas fuentes de manera eficiente, evitando duplicados y facilitando la identificación de fuentes sospechosas.

La eficiencia de los conjuntos también se ve en su capacidad para realizar operaciones rápidas como la adición, eliminación y verificación de la existencia de un elemento. Esto es vital en entornos donde la velocidad de respuesta es crítica. Por ejemplo, si un conjunto de direcciones IP conocidas por ser parte de una red de bots se actualiza constantemente, un sistema puede verificar rápidamente si una dirección IP sospechosa está en este conjunto.

Además, los conjuntos pueden ser utilizados para comparar y contrastar diferentes grupos de datos. Por ejemplo, comparar conjuntos de direcciones IP normales contra direcciones IP asociadas con comportamientos maliciosos puede revelar patrones y ayudar a mejorar las estrategias de seguridad.

En conclusión, los conjuntos son herramientas valiosas en la detección de accesos maliciosos. Su capacidad para manejar elementos únicos y realizar operaciones rápidas los hace esenciales para identificar y responder a amenazas de seguridad, particularmente en el contexto de las redes de bots. Combinados con otras estrategias y tecnologías, pueden jugar un papel crucial en la protección de sistemas y redes contra ataques cibernéticos.