Tec de Monterrey Campus Santa Fe

Programación de Estructura de Datos y Algoritmos Fundamentales

Actividad 5.2 Reflexión

Profesor:

Vicente Cubells

Alumnos:

Paúl Araque Fernández A01027626

Fecha de entrega:

27 Noviembre 2023

Preguntas:

1. **Hay algún nombre de dominio en el conjunto que sea anómalo (Esto puede ser con inspección visual).**

Sitio: kdkkgs7z6ptuhv2f8jub.ru

Sitio: nyvbcosk2llkngjncf9o.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?**

Sitio: kdkkgs7z6ptuhv2f8jub.ru ---> IP: 68.25.108.136

Sitio: nyvbcosk2llkngjncf9o.net ---> IP: 191.42.39.21

Se contesto la pregunta 1 y 2 en un mismo mapa cuya clave era el nombre y el valor era la IP entonces siendo dos preguntas en un mismo código se mejora la complejidad. No tuvimos que iterar sobre el vector de los registros dos veces.

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.**

La cantidad de IPs pertenecientes al dominio 'reto.com' que tienen al menos una conexión entrante son: 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.**

Estas son las 10 IPs seleccionadas:

172.17.230.1

172.17.230.10

172.17.230.2

172.17.230.3

172.17.230.4

172.17.230.5

172.17.230.6

172.17.230.7

172.17.230.8

172.17.230.9

IPs únicas de las Conexiones Entrantes:

172.17.230.49

5. **Considerando el resultado de las preguntas 3 y 4, ¿Qué crees que esté ocurriendo en esta red? (Pregunta sin código)**

Alta Cantidad de IPs con Conexiones Entrantes: El hecho de que 253 de las IPs posibles en el dominio reto.com tengan al menos una conexión entrante es significativo. Esto sugiere que casi todas las computadoras en la red están activas y recibiendo conexiones. Esto puede ser normal en una red grande y activa, pero también podría ser un indicio de actividad inusual,

como un escaneo de red o intentos de conexión automatizados (por ejemplo, en el contexto de un ataque cibernético).

Concentración de Conexiones Entrantes en una Única IP: El hecho de que, de las 10 IPs seleccionadas que no son el servidor ni el DHCP, todas las conexiones entrantes únicas vayan dirigidas a una sola IP (172.17.230.49) es bastante inusual. Esto podría indicar que esta IP específica está ofreciendo un servicio crítico o popular dentro de la red, o que está siendo el objetivo de un tipo específico de tráfico, malintencionado.

Actividad Maliciosa: Esta concentración de tráfico podría indicar un comportamiento sospechoso, como un ataque de Denegación de Servicio Distribuido (DDoS) contra esa IP, o que esta IP actúe como un punto de control en un ataque de red, como un servidor de comando y control en una botnet.

En conlcusión podemos observar que de las 10 IP's pruebas la única IP única que existía es la 172.17.230.49 lo que nos hace creer que esta computadora fue la primera en infectarse y es la que esta infectando a las otras computadoras.

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

Hay conexion entre la IP única 172.17.230.49 y el nombre kdkkgs7z6ptuhv2f8jub.ru
Hay conexion entre la IP única 172.17.230.49 y el nombre nyvbcosk2llkngjncf9o.net

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.**

Primera comunicación entre las IPs únicas y las computadoras anómalas:
La primera conexión entre las IPs únicas y las computadoras con nombres anómalos se realizó en la fecha 17-8-2020 a la computadora nyvbcosk2llkngjncf9o.net a través del puerto 443
Primera comunicación entre las IPs únicas y la computadora kdkkgs7z6ptuhv2f8jub.ru:
La primera conexión entre las IPs únicas y la computadora kdkkgs7z6ptuhv2f8jub.ru se realizó en la fecha 17-8-2020 a través del puerto 443
Primera comunicación entre las IPs únicas y la computadora nyvbcosk2llkngjncf9o.net:
La primera conexión entre las IPs únicas y la computadora nyvbcosk2llkngjncf9o.net se realizó en la fecha 17-8-2020 a través del puerto 443

El protocolo usado es el puerto destino: 443 que pertenece a un sitio web

Reflexión:

En esta actividad tenemos un escenario complejo de actividad de red, que involucra tanto la identificación de dominios y direcciones IP anómalas como el análisis de patrones de tráfico dentro de una red empresarial. La eficiencia y la importancia del uso de conjuntos (sets) y diccionarios (hash maps) en este contexto se pueden analizar desde varias perspectivas:

Importancia y Eficiencia de los Conjuntos

1. Prevención de Duplicados:

- Importancia: Los conjuntos son cruciales para asegurar que cada elemento sea único, lo cual es esencial cuando se identifican nombres de dominio anómalos. Esto evita el procesamiento redundante y garantiza que el análisis se centre en elementos distintos.

- Eficiencia: Al agregar automáticamente solo elementos únicos, los conjuntos ahorran tiempo y recursos computacionales, ya que no se requiere verificar manualmente la existencia de duplicados antes de cada inserción.

2. Rápida Verificación de Existencia:

- Importancia: En la seguridad de la red, la capacidad de verificar rápidamente si un dominio o una IP específica está presente en un conjunto es vital para la detección oportuna de actividades sospechosas.

- Eficiencia: Los conjuntos, implementados comúnmente como tablas hash, permiten una verificación casi instantánea de la existencia de un elemento, con una complejidad temporal promedio de O(1).

Importancia y Eficiencia de los Diccionarios (Hash Maps)

1. Asociación Clave-Valor:

- Importancia: Los diccionarios permiten asociar nombres de dominio con sus respectivas direcciones IP, facilitando un acceso rápido a la información relevante. Esto es crucial para mapear rápidamente los dominios identificados a sus IPs correspondientes.

- Eficiencia: Al igual que los conjuntos, los diccionarios ofrecen una complejidad temporal promedio de O(1) para inserciones, búsquedas y eliminaciones, lo que los hace extremadamente eficientes para el procesamiento de grandes volúmenes de datos.

2. Rápida Recuperación de Datos:

- Importancia: En el análisis de seguridad, poder recuperar rápidamente la dirección IP asociada con un nombre de dominio sospechoso es fundamental para investigar y responder a incidentes de seguridad.

- Eficiencia: La recuperación de datos basada en la clave (nombre del dominio) es muy rápida en los diccionarios, lo que permite un análisis eficiente incluso en situaciones de tiempo crítico.

Reflexión General

El uso de conjuntos y diccionarios en el análisis de redes es un ejemplo claro de cómo la elección adecuada de estructuras de datos puede tener un impacto significativo en la eficiencia y efectividad del procesamiento de datos. En el contexto de la seguridad de la red, donde la rapidez y la precisión son cruciales, estas estructuras ofrecen las herramientas necesarias para manejar grandes conjuntos de datos de manera eficiente, permitiendo a los analistas centrarse en la interpretación de los datos en lugar de preocuparse por los detalles de su gestión.

En este caso, la identificación de patrones anómalos de tráfico y la rápida asociación entre nombres de dominio y direcciones IP son facilitados enormemente por el uso de

conjuntos y diccionarios, lo que subraya la importancia de una sólida comprensión de las estructuras de datos en el campo de la seguridad informática.