José Leobardo Navarro Márquez

A01541324

Investigación y Reflexión: Uso de Grafos y Listas de Adyacencia en la Detección de Ataques Cibernéticos

La detección de patrones de ataque es fundamental para prevenir accesos no autorizados. En este trabajo, utilizamos una lista de adyacencia como estructura de datos para modelar ataques a puertos en horarios sospechosos (00:00 - 05:00). Nuestro objetivo fue encontrar el puerto con el mayor fan-out, es decir, el que fue atacado por la mayor cantidad de direcciones IP distintas. Esto permitió identificar posibles ataques coordinados y determinar si existía un bot master controlando los intentos de acceso.

Una lista de adyacencia es una representación eficiente de un grafo en el que cada nodo (puerto) está asociado con un conjunto de nodos adyacentes (IPs que lo atacaron). Esta estructura nos permitió:

- Almacenar de manera eficiente las conexiones IP-Puerto sin desperdicio de memoria.
- Acceder rápidamente a la información sobre qué IPs intentaron acceder a cada puerto.
- Identificar el puerto con mayor fan-out, es decir, aquel que presentó intentos de acceso desde la mayor cantidad de IPs distintas.

Puerto con Mayor Fan-Out

Para identificar el puerto más atacado en horas sospechosas, seguimos estos pasos:

Construcción de la lista de adyacencia:

Se extrajo la información de cada registro de bitácora.

Se identificó el puerto objetivo de cada intento de acceso.

Se almacenaron las IPs que intentaron conectarse a cada puerto.

Cálculo del fan-out por puerto:

Se contó cuántas IPs diferentes estaban asociadas a cada puerto en la lista de adyacencia.

Se identificó el puerto con la mayor cantidad de IPs atacantes distintas.

Identificación del posible bot master:

Se revisaron los registros asociados al puerto con mayor fan-out.

Si una IP intentó acceder con credenciales como "admin" y se marcó como posible bot master

Este enfoque basado en grafos demostró ser eficiente y preciso en la detección de patrones de ataque. Al analizar la cantidad de IPs atacantes por puerto, pudimos determinar no solo el punto de acceso más vulnerable, sino también identificar posibles intentos de control de una botnet. Implementar estructuras de grafos en ciberseguridad permite detectar ataques antes de que generen un impacto crítico, mejorando la protección de los sistemas y previniendo accesos no autorizados. Hay áreas de oportunidad como analizar los octetos de cada ip para determinar una posible misma subred, pero considerando los datos que tenemos es la solución más precisa que pudimos encontrar.