“Instituto Tecnológico y estudios superiores de Monterrey”

EVIDENCIA

“Reflexión Actividad 3.3”

Materia:
Programación de estructuras de datos y algoritmos fundamentales
(Gpo 570)

Profesor:
Dr. Eduardo Arturo Rodríguez Tello

Alumno/a:
Ayetza Yunnuen Infante García | A01709011
Luis Carlos Rico Almada | A01252831

22/Julio/2023

Ayetza Yunnuen Infante García | A01709011

Las estructuras de datos jerárquicas son fundamentales para resolver problemas complejos y organizar datos de manera eficiente. En el contexto de una situación problema relacionada con registros de bitácoras de red, estas estructuras pueden ser de gran utilidad para el análisis y la detección de posibles infecciones en una red *(W, Anggoro; s.f)*.

Una estructura de datos jerárquica es una colección de elementos organizados en forma de árbol, donde cada elemento tiene un nodo padre (excepto el nodo raíz) y cero o más nodos hijos. En el caso de las bitácoras de red, estas estructuras pueden ser representadas mediante árboles, donde la raíz es un registro general y los registros más detallados están en niveles inferiores del árbol *(Universidad de Cantabria, 2009)*.

La importancia de utilizar estructuras de datos jerárquicas radica en que permiten organizar y representar de manera eficiente la información de los registros de la red, lo que facilita la búsqueda, filtrado, análisis y la detección de patrones anómalos *(Geek for Geeks, 2016)*. Las estructuras jerárquicas permiten realizar búsquedas más rápidas y eficientes, ya que al estar organizadas en forma de árbol, se puede aplicar búsqueda binaria o búsqueda por índices, reduciendo el tiempo de búsqueda y análisis de datos; de igual forma mediante el análisis de los registros en diferentes niveles del árbol, se pueden identificar patrones y tendencias de comportamiento en la red, lo que facilita la detección de actividad sospechosa o inusual. Con una estructura jerárquica bien definida, es más sencillo identificar conexiones y secuencias de eventos que podrían indicar una infección en la red. Por ejemplo, la detección de múltiples intentos de inicio de sesión fallidos o patrones de tráfico inusuales podrían ser indicios de una intrusión *(B, Reiter; R, Rivera. 2013)*.

La estructura jerárquica permite organizar los registros de manera eficiente, lo que implica un menor consumo de recursos y una mayor velocidad en la manipulación de datos; al igual que son escalables, lo que significa que pueden adaptarse a la adición de nuevos registros sin perder eficiencia. Esto es especialmente útil en entornos de red que generan grandes volúmenes de datos constantemente *(R, Woehrer, S, & Woehrer, S. 2017)*.

Para determinar si una red está infectada o no, se pueden aplicar diversas técnicas y algoritmos en función de los datos disponibles y la estructura de la red. Algunas estrategias comunes incluyen:

1. Análisis de Comportamiento: Mediante el análisis de patrones y comportamientos anómalos en los registros, se pueden identificar actividades sospechosas, como accesos no autorizados o intentos de acceso repetidos *(R, Adeva 2015)* .

2. Análisis de Tráfico: Monitorizar el tráfico de red y detectar patrones inusuales o picos de actividad que puedan indicar una infección o una campaña de ataque *(R, Adeva 2015).*

3. Organización de la Información: Las estructuras de datos jerárquicas, como los árboles, permiten organizar los registros de bitácoras o eventos de la red en una estructura lógica y ordenada. Cada nodo del árbol representa un registro con información detallada, y los nodos se conectan según su relevancia o relación. Esta organización facilita la navegación y búsqueda de información, lo que es esencial para analizar grandes volúmenes de registros en tiempo real *(M, Liberatori; 2018)*.

4. Análisis de Vulnerabilidades: Identificar vulnerabilidades conocidas en los sistemas y aplicaciones de la red que puedan ser explotadas por malware *(M, Liberatori; 2018)*..

5. Detección de anomalías: Emplear técnicas de detección de anomalías para identificar comportamientos inusuales en el tráfico de red o en los registros de eventos *(M, Liberatori; 2018)*.

En conclusión, las estructuras de datos jerárquicas son esenciales para organizar y analizar registros de bitácoras de red de manera eficiente. Su uso adecuado facilita la detección de patrones, comportamientos anómalos y posibles infecciones en la red, permitiendo una respuesta más rápida y efectiva ante amenazas potenciales. La combinación de técnicas de análisis y detección con estructuras jerárquicas bien diseñadas es fundamental para mantener la seguridad de una red y protegerla contra posibles ataques informáticos.

Luis Carlos Rico Almada | A01252831

En el contexto de las redes informáticas y la seguridad de la información, la detección temprana de posibles infecciones o intrusiones es de vital importancia para evitar daños y mantener la integridad de los sistemas. Una de las técnicas ampliamente utilizadas para determinar si una red está infectada o no es el análisis de registros de eventos o bitácoras (logs) *(K.Furlinger, C. Glass, J. Gracia s.f)*.

Las bitácoras de red registran información detallada sobre las actividades y eventos que ocurren en una red, como intentos de inicio de sesión, transferencia de datos, acceso a recursos compartidos, etc. El análisis de estas bitácoras es fundamental para identificar patrones de comportamiento sospechoso o inusual que puedan indicar una posible infección *(Alcaldía Mayor de Bogotá 2017)*.

Una estrategia efectiva para determinar si una red está infectada o no es utilizar el enfoque de "detección de anomalías". Este método consiste en analizar los registros en busca de actividades que se desvíen significativamente del comportamiento normal de la red. Algunas consideraciones clave para llevar a cabo esta detección son:

1. Perfil del Comportamiento Normal: Es necesario establecer un perfil del comportamiento normal de la red. Esto implica analizar las bitácoras durante un período de tiempo representativo para entender cómo debería comportarse la red en situaciones normales *(E, Vega. 2021)*.

2. Uso de Algoritmos de Detección de Anomalías: Existen diversos algoritmos de detección de anomalías, como el "análisis de componentes principales" (PCA), "bosques aleatorios" (Random Forests), "detección de valores atípicos" (Outlier Detection), entre otros. Estos algoritmos pueden aplicarse a las bitácoras para identificar comportamientos inusuales *(Sushir, T. s.f)*.

3.Monitoreo Continuo:La detección de anomalías debe ser un proceso continuo y en tiempo real. Es fundamental tener sistemas que monitorean constantemente las bitácoras y generen alertas ante eventos sospechosos *(Sushir, T. s.f)*.

4. Integración de Contexto. Es importante considerar el contexto de la red y el entorno en el que se encuentran los sistemas. Lo que puede ser una anomalía en una red puede ser normal en otra. Por lo tanto, se deben considerar factores como la arquitectura de red, los patrones de tráfico habituales y las políticas de seguridad establecidas *(E, Vega. 2021)*.

5. Colaboración e Inteligencia Colectiva: La colaboración con fuentes externas de inteligencia de amenazas (por ejemplo, bases de datos de firmas de malware conocido) puede fortalecer la capacidad de detección de anomalías *(E, Vega. 2021)*.

Como conclusión, las estructuras de datos jerárquicas juegan un papel esencial en la detección de infecciones en redes informáticas. La eficiencia en la organización y análisis de datos, la detección de patrones y anomalías, y la capacidad de adaptarse a cambios en la red hacen que estas estructuras sean fundamentales para proteger la integridad y seguridad de los sistemas. Combinadas con técnicas de análisis y algoritmos de detección, las estructuras jerárquicas permiten una respuesta más rápida y efectiva ante posibles amenazas, fortaleciendo la defensa y protección de las redes contra ataques informáticos.

Referencias

W, Anggoro (s.f) *C++ Data Structures and Algorithms* ORREILLY
https://www.oreilly.com/library/view/c-data-structures/9781788835213/5846efc4-7a45-4c45-bc1f-fec1dfde85bd.xhtml

M. Harbour (2009) *Estructuras de Datos y Algoritmos* Universidad de Cantabria.
https://www.ctr.unican.es/asignaturas/eda/cap3-jerarquicos-2en1.pdf

GeeksforGeeks (2016) *Introduction to Hierarchical Data Structure*.
https://www.geeksforgeeks.org/introduction-to-hierarchical-data-structure/

B, Reiter; R, Rivera. (2013) *Hierarchical Data Structures and Related Concepts for the C++* Standard Library https://www.open-std.org/jtc1/sc22/wg21/docs/papers/2013/n3700.html

R, Woehrer, S, & Woehrer, S. (2017). *Representing hierarchical data* (C++).
https://softwareengineering.stackexchange.com/questions/344174/representing-hierarchical-data-c

R, Adeva (2015) *¿Cómo saber si nuestro router tiene malware y cómo evitarlo?* Smart Life
https://cincodias.elpais.com/cincodias/2015/08/31/lifestyle/1441030486_670198.html

M, Liberatori (2018) *Redes de Datos y sus Protocolos* Universidad Nacional de Mar del Plata EUDEM
http://www2.mdp.edu.ar/images/eudem/pdf/redes%20de%20datos.pdf

K.Furlinger, C. Glass, J. Gracia (s.f) *DASH: Data Structures and Algorithms with Support for Hierarchical Locality* Ludwig-Maximilians-Universit¨at (LMU) Munich Computer Science Department, MNM Team
https://link.springer.com/content/pdf/10.1007/978-3-319-14313-2_46.pdf

Alcaldía Mayor de Bogotá (2017) *Gestión de Incidentes de Seguridad de la Información* IPES
https://www.ipes.gov.co/images/informes/SDE/Mapa_de_Procesos/Proceso_Gestion_de_seguridad_de_la_Informacion_y_Recursos_Tecnologicos/2020/In_069_Gestion_De_Incidentes_De_Seguridad.pdf.pdf

E, Vega. (2021) *Seguridad de la Información* 3Ciencias
https://www.3ciencias.com/wp-content/uploads/2021/03/LIBRO-SEGURIDAD-INFORMACIO%CC%81N.pdf

Sushir, T. (s.f). *Detección de anomalías: guía para prevenir intrusiones en la red*.
https://geekflare.com/es/anomaly-detection/