PUCE Virtual

DOCUMENTO DE PROFUNDIZACIÓN

Programación III

Estudio de caso 1: Selección de Estructuras de Datos

Estudio de caso 1: Selección de Estructuras de Datos

Contexto

En los sistemas de ciberseguridad actuales, se procesan grandes volúmenes de datos provenientes de logs, eventos de red y actividades de usuarios. La eficiencia en el manejo de esta información depende en gran medida de la correcta selección de estructuras de datos, ya que estas influyen directamente en el rendimiento, la velocidad de respuesta y el uso de recursos del sistema.

Problema

Una organización necesita desarrollar un sistema que permita analizar eventos de seguridad en tiempo real para detectar intentos de acceso no autorizado. El sistema debe procesar miles de registros por segundo, permitiendo búsquedas rápidas, bajo consumo de memoria y escalabilidad.

Solución Propuesta

Seleccionar estructuras de datos que optimicen el acceso y procesamiento de la información. En este caso, se propone el uso de tablas hash para búsquedas rápidas y listas para almacenamiento temporal de eventos.

Estrategia:

- Analizar los requerimientos del sistema (velocidad, volumen de datos).
- Evaluar distintas estructuras (listas, árboles, grafos, hash).
- Seleccionar la combinación que mejor equilibre rendimiento y consumo de recursos.

Implementación

```
# Simulación de análisis de eventos de seguridad
logs = ["login_ok", "login_fail", "login_fail", "intrusion", "login_ok"]

contador = {}

for evento in logs:
    if evento in contador:
        contador[evento] += 1
    else:
        contador[evento] = 1

# Identificar eventos sospechosos
```

```
for evento, cantidad in contador.items():
    if evento == "login_fail" and cantidad > 1:
        print("Alerta: múltiples intentos fallidos")
```

Resultados e Impacto en ciberseguridad

El uso de tablas hash permite una búsqueda eficiente en tiempo constante, mejorando la detección de patrones sospechosos en grandes volúmenes de datos. Esto reduce el tiempo de respuesta ante amenazas y mejora la capacidad de monitoreo en tiempo real.

Reflexión Técnica

La selección de estructuras de datos no debe basarse únicamente en la facilidad de implementación, sino en un análisis técnico que considere rendimiento, escalabilidad y contexto. En ciberseguridad, una elección adecuada puede marcar la diferencia entre detectar una amenaza a tiempo o no, evidenciando la importancia de tomar decisiones fundamentadas en el diseño del sistema.