PUCE Virtual

DOCUMENTO DE PROFUNDIZACIÓN

Programación III

Laboratorio de Contenido 3:

Explicación básica

En ciberseguridad, los grafos ponderados se utilizan para analizar redes informáticas y evaluar posibles rutas de ataque. En este caso, el peso de una conexión puede representar el nivel de vulnerabilidad, la dificultad del ataque o el impacto potencial de comprometer un sistema. Gracias a estos valores, los analistas de seguridad pueden identificar cuáles son los caminos más probables o peligrosos que un atacante podría utilizar para desplazarse dentro de una red.

Objetivos

- Comprender el concepto de grafo ponderado.
- Identificar cómo se representan los pesos en las aristas.
- Analizar rutas dentro de una red informática.
- Determinar rutas de ataque con menor o mayor costo.
- Implementar un grafo ponderado utilizando Python.

Caso práctico

Una empresa desea analizar la seguridad de su infraestructura de red. Los analistas han identificado diferentes sistemas y el nivel de dificultad que tendría un atacante para moverse entre ellos.

Los sistemas identificados son:

- Internet
- Firewall
- Servidor Web
- Servidor de Aplicaciones
- Base de Datos

Cada conexión tiene un peso que representa la dificultad del ataque (entre menor sea el número, más fácil sería comprometer el sistema).

Conexión	Dificultad del ataque
Internet → Firewall	3
Firewall → Servidor Web	2
Servidor Web → Servidor Aplicaciones	2
Servidor Aplicaciones → Base de Datos	4

Problema

El equipo de seguridad desea analizar cuál sería la ruta más sencilla para que un atacante comprometa la base de datos si logra entrar desde Internet.

Para ello se requiere:

- Representar la red como un grafo ponderado.
- Calcular el costo total de las rutas posibles.
- Identificar la ruta de menor dificultad para el atacante.

Aplicación paso a paso

Paso 1: Identificar los nodos

Los nodos representan los sistemas de la red:

- Internet
- Firewall
- Servidor Web
- Servidor de Aplicaciones
- Base de Datos

Paso 2: Definir las conexiones con pesos

Cada conexión tendrá un valor que representa el nivel de dificultad del ataque.

Ejemplo:

Internet → Firewall (3)
Firewall → Servidor Web (2)
Servidor Web → Servidor Aplicaciones (2)
Servidor Aplicaciones → Base de Datos (4)

Paso 3: Representar el grafo en Python

El grafo puede representarse utilizando **diccionarios con pesos asociados**.

Implementación en Python

```python
import heapq

# Grafo ponderado representado como diccionario
grafo = {
    "Internet": {"Firewall": 3},
    "Firewall": {"Servidor Web": 2},
    "Servidor Web": {"Servidor Aplicaciones": 2},
    "Servidor Aplicaciones": {"Base de Datos": 4},
    "Base de Datos": {}
}
def dijkstra(grafo, inicio):
    distancias = {nodo: float('inf') for nodo in grafo}
    distancias[inicio] = 0
    cola = [(0, inicio)]

    while cola:
        distancia_actual, nodo_actual = heapq.heappop(cola)

        for vecino, peso in grafo[nodo_actual].items():
            distancia = distancia_actual + peso

            if distancia < distancias[vecino]:
                distancias[vecino] = distancia
                heapq.heappush(cola, (distancia, vecino))

    return distancias

resultado = dijkstra(grafo, "Internet")

print("Costo mínimo para llegar a cada sistema:")
for nodo, costo in resultado.items():
    print(nodo, ":", costo)
```

Conclusiones

Los grafos ponderados permiten representar redes informáticas donde las conexiones tienen diferentes niveles de costo, riesgo o dificultad. En ciberseguridad, esta característica es muy útil para analizar rutas de ataque potenciales y comprender qué sistemas podrían ser más vulnerables dentro de una infraestructura.

En este laboratorio se observó cómo una red puede modelarse mediante un grafo ponderado y cómo es posible calcular rutas utilizando algoritmos como Dijkstra. Este tipo

de análisis permite a los especialistas en seguridad identificar los caminos más críticos que un atacante podría aprovechar.

El uso de grafos ponderados facilita la evaluación de riesgos, la priorización de medidas de seguridad y el diseño de estrategias de defensa, contribuyendo a mejorar la protección de los sistemas y redes informáticas.