PUCE Virtual

DOCUMENTO DE PROFUNDIZACIÓN

Programación III

Laboratorio de Contenido 2:

Laboratorio de Contenido 2:

Explicación básica

En ciberseguridad, los grafos dirigidos son especialmente útiles para representar flujos de comunicación, rutas de ataque y dependencias entre sistemas. Por ejemplo, pueden modelar cómo un atacante se mueve dentro de una red, comenzando desde un equipo comprometido y avanzando hacia servidores o bases de datos.

Este tipo de representación facilita el análisis de posibles vulnerabilidades, la identificación de rutas críticas y la comprensión del comportamiento de la red.

Objetivos

- Comprender el concepto de grafo dirigido.
- Identificar los componentes principales de un grafo.
- Representar relaciones entre sistemas mediante grafos dirigidos.
- Analizar posibles rutas de ataque en una red.
- Implementar un grafo dirigido utilizando Python.

Caso práctico

Una organización desea analizar cómo un atacante podría desplazarse dentro de su red interna.

La infraestructura simplificada es la siguiente:

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

El flujo de acceso dentro de la red puede representarse de la siguiente forma:

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

Cada conexión tiene una **dirección**, ya que el acceso ocurre siguiendo un flujo específico dentro de la red.

Problema

El equipo de seguridad desea analizar las posibles rutas que un atacante podría seguir dentro de la red si logra comprometer un punto inicial.

Se requiere:

- Representar la infraestructura como un grafo dirigido.
- Analizar las rutas posibles desde un nodo inicial.
- Simular el recorrido del atacante dentro del sistema.

Aplicación paso a paso

Paso 1: Identificar los nodos

Los nodos del grafo serán:

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

Paso 2: Identificar las conexiones dirigidas

Las conexiones representan el flujo de acceso dentro de la red.

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

Paso 3: Representar el grafo

El grafo puede representarse mediante una **lista de adyacencia**, que es una estructura común en programación.

Implementación en Python

```python
grafo = {
    "Internet": ["Firewall"],
    "Firewall": ["Servidor Web"],
    "Servidor Web": ["Servidor Aplicaciones"],
    "Servidor Aplicaciones": ["Base de Datos"],
    "Base de Datos": []
}

# Función para recorrer el grafo (búsqueda en profundidad)
def dfs(nodo, visitados):
    if nodo not in visitados:
        print(nodo)
        visitados.add(nodo)

        for vecino in grafo[nodo]:
            dfs(vecino, visitados)

# Simulación del recorrido de un atacante
print("Ruta potencial de ataque:")

dfs("Internet", set())
```

Conclusiones

En ciberseguridad, los grafos facilitan la comprensión de cómo un atacante podría desplazarse dentro de una infraestructura tecnológica.

A través de este laboratorio se observó cómo una red puede representarse mediante un grafo dirigido y cómo es posible analizar rutas de acceso utilizando algoritmos de recorrido.

La implementación en Python demuestra que estas estructuras pueden utilizarse para simular escenarios de ataque y estudiar posibles vulnerabilidades.

El uso de grafos dirigidos ayuda a los analistas de seguridad a identificar rutas críticas, detectar posibles puntos de intrusión y mejorar las estrategias de defensa, fortaleciendo así la seguridad de los sistemas informáticos.