PUCE Virtual

DOCUMENTO DE PROFUNDIZACIÓN

Programación III

Laboratorio de Contenido 1: Árbol de decisión aplicado a ciberseguridad

Laboratorio de Contenido 1: Árbol de decisión aplicado a ciberseguridad

Explicación básica

Un árbol de ataque es un modelo utilizado en ciberseguridad para representar de forma estructurada las distintas formas en que un atacante puede comprometer un sistema. En este modelo, el objetivo principal del atacante se coloca en el nodo raíz del árbol, mientras que los nodos hijos representan las acciones o pasos necesarios para alcanzar ese objetivo.

Los árboles de ataque permiten descomponer un ataque complejo en pasos más pequeños y analizables. Además, ayudan a identificar vulnerabilidades, priorizar medidas de seguridad y evaluar riesgos dentro de una infraestructura informática.

Objetivos

- Comprender el concepto de árbol de ataque.
- Identificar los componentes principales de un árbol de ataque.
- Analizar escenarios básicos de ataques informáticos.
- Representar un árbol de ataque mediante una estructura de datos.
- Implementar un ejemplo sencillo de árbol de ataque en Python.

Caso práctico

Una empresa posee un servidor web interno que almacena información importante. El equipo de seguridad desea analizar cómo un atacante podría comprometer dicho servidor.

El objetivo del atacante es: Comprometer el servidor web

Las posibles formas de lograrlo pueden ser:

1. Ataque de fuerza bruta para obtener credenciales.
2. Explotación de una vulnerabilidad del sistema.
3. Phishing dirigido al administrador del sistema.

Esto puede representarse mediante un árbol de ataque.

- Comprometer servidor web
- Fuerza bruta
- Exploit vulnerabilidad
- Phishing al administrador

Problema

El departamento de seguridad desea modelar las posibles rutas de ataque contra su servidor web para identificar riesgos potenciales.

Se requiere:

- Representar el árbol de ataque mediante una estructura de datos.
- Mostrar los posibles caminos que un atacante podría utilizar.
- Implementar una simulación simple utilizando Python.

Aplicación paso a paso

Paso 1: Definir el objetivo del ataque

El nodo raíz será:

Comprometer servidor web

Paso 2: Identificar los métodos de ataque

Se identifican tres métodos principales:

- Fuerza bruta
- Exploit de vulnerabilidad
- Phishing

Paso 3: Representar el árbol

El árbol puede representarse mediante nodos y subnodos.

Comprometer servidor

* Fuerza bruta
    └── Adivinar contraseña
* Exploit vulnerabilidad
    └── Vulnerabilidad en software
* Phishing
    └── Engañar administrador

Paso 4: Modelar la estructura en Python

Cada nodo del árbol representará una acción dentro del ataque.

Implementación en Python

```python
class NodoAtaque:
    def __init__(self, nombre):
        self.nombre = nombre
        self.hijos = []

    def agregar_hijo(self, nodo):
        self.hijos.append(nodo)

def mostrar_arbol(nodo, nivel=0):
    print(" " * nivel + "- " + nodo.nombre)
    for hijo in nodo.hijos:
        mostrar_arbol(hijo, nivel + 4)
```

```python
# Crear nodo raíz
raiz = NodoAtaque("Comprometer servidor web")

# Crear nodos de ataque
fuerza_bruta = NodoAtaque("Ataque de fuerza bruta")
exploit = NodoAtaque("Exploit de vulnerabilidad")
phishing = NodoAtaque("Phishing al administrador")

# Subataques
adivinar = NodoAtaque("Adivinar contraseña")
vulnerabilidad = NodoAtaque("Explotar vulnerabilidad del software")
engaño = NodoAtaque("Enviar correo de phishing")

# Construir árbol
raiz.agregar_hijo(fuerza_bruta)
raiz.agregar_hijo(exploit)
raiz.agregar_hijo(phishing)

fuerza_bruta.agregar_hijo(adivinar)
exploit.agregar_hijo(vulnerabilidad)
phishing.agregar_hijo(engaño)

# Mostrar árbol
mostrar_arbol(raiz)
```

Conclusiones

Los árboles de ataque son herramientas muy útiles para analizar amenazas dentro de un sistema informático. Permiten representar de forma clara los distintos caminos que un atacante podría seguir para comprometer una infraestructura tecnológica.

A través de este laboratorio se pudo observar cómo un escenario de ataque puede dividirse en diferentes etapas y cómo estas pueden modelarse mediante una estructura jerárquica. Además, se demostró que es posible implementar este tipo de modelos utilizando Python, lo que facilita la simulación y análisis de escenarios de seguridad.

El uso de árboles de ataque ayuda a los analistas de seguridad a identificar vulnerabilidades, evaluar riesgos y diseñar estrategias de defensa más efectivas, contribuyendo a mejorar la protección de los sistemas informáticos.