DOCUMENTO DE PROFUNDIZACIÓN

Programación III

Laboratorio de Contenido 1: Modelado de Infraestructuras de Red

Laboratorio de Contenido 1: Modelado de Infraestructuras de Red

Explicación básica

El modelado de infraestructuras de red consiste en representar los distintos componentes de una red informática (como routers, servidores, dispositivos y conexiones) mediante estructuras de datos, especialmente grafos. En este modelo, los nodos representan los dispositivos o activos, mientras que las aristas representan las conexiones o flujos de comunicación. Este enfoque permite analizar la topología de la red, identificar vulnerabilidades y comprender cómo se propaga la información o posibles amenazas dentro del sistema.

Objetivos

- Comprender cómo se modela una red utilizando grafos.
- Identificar los elementos clave de una infraestructura tecnológica.
- Analizar relaciones y dependencias dentro de una red.
- Aplicar el modelo en un escenario de ciberseguridad.

Caso práctico

Una empresa desea analizar su red interna para identificar posibles rutas de ataque y mejorar su seguridad.

Problema

Se cuenta con los siguientes elementos:

- Dispositivos: PC1, PC2, Servidor, Router, Firewall
- Conexiones entre ellos

Se requiere:

- Representar la red.
- Identificar conexiones críticas.
- Analizar posibles rutas de acceso no autorizado.

Aplicación paso a paso

Paso 1: Definir nodos y conexiones

Identificar los dispositivos y cómo están conectados.

Paso 2: Modelar con grafo en Python

```
import networkx as nx

G = nx.Graph()

# Nodos
dispositivos = ["PC1", "PC2", "Servidor", "Router", "Firewall"]
G.add_nodes_from(dispositivos)

# Conexiones
G.add_edges_from([
  ("PC1", "Router"),
  ("PC2", "Router"),
  ("Router", "Firewall"),
  ("Firewall", "Servidor")
])

print("Conexiones:", G.edges())
```

Paso 3: Analizar la red

- Identificar nodos con más conexiones.
- Detectar posibles puntos críticos.

```
print(nx.degree_centrality(G))
```

Conclusiones

- El modelado de infraestructuras de red mediante grafos permite representar de forma clara y estructurada las relaciones entre los distintos componentes de un sistema.
- En ciberseguridad, este enfoque facilita la identificación de vulnerabilidades, rutas de ataque y nodos críticos, mejorando la toma de decisiones para proteger la infraestructura. Además, permite simular escenarios y evaluar el impacto de posibles incidentes antes de que ocurran.