Traffic Analyzer

Traffic Analyzer es una aplicación para capturar y analizar paquetes de red en tiempo real. Permite monitorear protocolos como TCP, UDP e ICMP, y genera estadísticas básicas sobre el tráfico capturado.

Requisitos Previos

Para Ejecución Local con Python

- Python 3.8 o superior** instalado en tu sistema.
- Instalación de la biblioteca **Scapy**:
    - [Instalación:] En CMD o Bash ejecutar el siguiente comando “pip install scapy”
- Instalación de **WinPcap y Npcap** (necesarios para capturar paquetes en sistemas Windows):
    - [WinPcap] (https://www.winpcap.org/install)
    - [Npcap] (https://nmap.org/npcap)

Ejecución con Docker

- Docker instalado en tu sistema.
- Configuración de privilegios de red para Docker.

Configuración y Ejecución

Modo Local (Python)

- Navega a la carpeta del proyecto:
    - CMD o Bash: cd ruta/del/proyecto
- Ejecuta el script principal:
    - CMD o Bash: python traffic_analyzer.py

La aplicación comenzará a capturar paquetes y mostrará información en tiempo real. Presiona Ctrl + C para detener la captura y ver las estadísticas.

Modo Docker

- Construye la imagen Docker:
    - CMD o Bash: docker build -t traffic_analyzer
- Ejecuta el contenedor:
    - CMD o Bash: docker run --rm --cap-add=NET_ADMIN --network host traffic_analyzer

Al igual que en el modo local, presiona Ctrl + C para detener la captura y ver las estadísticas.

Uso

Mientras la aplicación está en ejecución, capturará y mostrará información sobre los paquetes de red en tiempo real en este formato:

"Paquete IPv4 de origen: [IP_ORIGEN] -> Destino: [IP_DESTINO] | Protocolo: [PROTOCOLO] - - Presionar (Ctrl + C) para mostrar estadísticas"

Al detener la aplicación, se generará un resumen como este:

--- Estadísticas de Tráfico ---

Total de paquetes capturados: 100

Paquetes por protocolo:

TCP: 70

UDP: 20

ICMP: 10

Top 5 IPs de origen:

192.168.1.10: (40 paquetes)

192.168.1.20: (30 paquetes)

Top 5 IPs de destino:

8.8.8.8: (50 paquetes)

192.168.1.1: (30 paquetes)

Archivos del Proyecto

traffic_analyzer.py: Script principal que captura y analiza el tráfico.

Dockerfile: Archivo para construir y ejecutar la aplicación en un contenedor Docker.

traffic_analyzer.bat: Ejecuta el scrip principal localmente (Windows)

traffic_analyzer.sh: Ejecuta el scrip principal localmente (Mac y Linux)

create_container.bat: Crea el contenedor (Windows)

create_container.sh: Crea el contenedor (Mac y Linux)

traffic_analyzer_Docker.bat: Ejecuta el contenedor de Docker (Windows)

traffic_analyzer_Docker.sh: Ejecuta el contenedor de Docker (Mac y Linux)

Notas

Permisos de Administrador: Para garantizar el correcto funcionamiento es recomendable ejecutar el script como administrador

Plataforma Recomendada para ejecutarlo en Docker: Aunque funciona en Windows, está pensada para ejecutarse en Linux y Mac.