Wireshark Network Tracking with Google Maps

Name: Abhik Das
Registration Number: 22BCE8616
College Email: abhik.22bce8616@vitapstudent.ac.in
Personal Email: abhikdas0811@gmail.com

Project Overview:

In the evolving landscape of cybersecurity, the ability to monitor and visualize network traffic in real-time has become crucial for identifying and mitigating potential threats. This project, titled "Wireshark Network Tracking with Google Maps," aims to provide an intuitive and visually driven solution to analyze network packet data and detect potentially malicious activities through geographical mapping. Built on Python and using Wireshark as the primary packet capture tool, the system empowers users to inspect IP addresses from network traffic and identify their physical locations on an interactive map. This helps in identifying attack origins, monitoring geographical trends, and enhancing forensic investigations.

Problem Statement:

Traditional packet analysis tools like Wireshark offer extensive raw data but lack visual context, especially when dealing with large-scale or real-time monitoring. There is a need for a tool that integrates geospatial awareness with network forensics to make threat detection faster and more intuitive. This project addresses the gap by creating a system that not only parses packet data but also maps it geographically and analyses the risk level of IP addresses using external threat intelligence APIs.

Tools and Technologies Used:

- **Programming Language:** Python
- **GUI Library:** Tkinter
- **Visualization Tools:** Folium for mapping, Matplotlib for data visualization
- **Threat Intelligence APIs:** AbuseIPDB, VirusTotal
- **Data Source:** Wireshark
- **Supporting Libraries:** pandas, geopy, requests

Existing System vs Proposed System:

The existing system, Wireshark, although powerful, provides a text-heavy interface and lacks real-time geolocation or threat intelligence capabilities. Analysts often need to manually interpret IP addresses, cross-reference external threat databases, and use separate tools for mapping.

The proposed system enhances this by integrating:

- **IP Geolocation:** Automated mapping of source/destination IPs on a world map.

- **Threat Analysis:** Real-time risk evaluation using APIs from AbuseIPDB and VirusTotal.
- **Visual Dashboards:** Protocol breakdowns, top malicious IPs, and threat summaries.
- **User Interface:** A simple Tkinter GUI for loading CSV files, filtering by country, and launching analytics.

System Design / Flow:

1. **Packet Capture:** Wireshark is used to monitor and export network packets in CSV format.
2. **File Import:** User selects the CSV file via the GUI.
3. **Parsing and Processing:** Data is cleaned and parsed using pandas.
4. **IP Analysis:** Source and destination IPs are extracted.
5. **Threat Verification:** IPs are checked via AbuseIPDB and VirusTotal APIs.
6. **Geolocation Mapping:** IP coordinates are retrieved and displayed using Folium maps.
7. **Analytics Dashboard:** Summary visuals (charts, graphs) are rendered using Matplotlib.

Expected Outcome / Conclusion:

This project is expected to yield a highly functional and user-friendly application that empowers cybersecurity professionals and researchers with a powerful tool for visualizing network threats. The mapping and analytics feature not only enhance situational awareness but also help in quick decision-making during incident response. By combining geolocation, real-time threat reputation scoring, and rich visual insights into one platform, the system stands as a robust enhancement over traditional network analysis tools. This project demonstrates a practical application of cybersecurity principles and data science in the realm of real-time network defense.
