**ScapyUI - Network Packet Sniffer**

**1. Introduction**

ScapyUI is a powerful graphical network packet sniffer built using **Scapy** and **Tkinter**. It provides a user-friendly interface for network analysis, allowing users to capture live network traffic, save packet data, and analyse **.pcap** files. This tool is designed for network forensics, penetration testing, and debugging purposes, supporting both **IPv4 and IPv6** protocols.

ScapyUI simplifies the process of analysing network traffic by displaying captured packets in categorized sections such as **packet summary, full packet dump, HTTP data, and DNS queries/responses**. Additionally, it features the ability to read and analyse .pcap files in a separate window for enhanced usability.

**2. Problem Statement**

Network traffic analysis is crucial for cybersecurity professionals, forensic investigators, and network administrators. Existing tools such as Wireshark provide extensive functionality but can be complex for beginners. Additionally, many open-source tools lack a structured GUI for easier analysis.

Key issues that ScapyUI aims to address:

* **Complexity of existing tools**: Advanced packet sniffers may overwhelm users with excessive details.
* **Lack of GUI-based solutions for Scapy**: While Scapy is a powerful Python library, it lacks a dedicated GUI for easier analysis.
* **Difficulty in .pcap analysis**: Users often struggle to interpret raw packet data efficiently.
* **Need for real-time monitoring**: A lightweight tool that can quickly display network traffic in categorized sections is highly valuable.

**3. Objectives**

The primary objectives of **ScapyUI** are:

1. **Provide an intuitive GUI** for network packet sniffing using **Scapy**.
2. **Enable real-time network traffic monitoring** with categorized packet information.
3. **Allow users to save packets to .pcap format** for further analysis.
4. **Provide functionality to open and analyse .pcap files** in a dedicated window.
5. **Support multiple network protocols** such as **TCP, UDP, ICMP, and DNS**.
6. **Extract and display HTTP and DNS traffic** separately for enhanced analysis.

**4. Proposed Methodology**

**4.1 Technology Stack**

ScapyUI is developed using the following technologies:

* **Python**: Core programming language.
* **Scapy**: Packet sniffing and analysis library.
* **Tkinter**: GUI development.
* **Threading**: Ensuring smooth performance by running packet capture in a separate thread.

**4.2 Implementation Details**

1. **Live Packet Capture**
   * Capture live packets using **Scapy’s sniffing capabilities**.
   * Display the data in categorized sections within the GUI.
2. **Packet Categorization**
   * Display different types of packets in separate sections (**Summary, Full Dump, HTTP, DNS**).
   * Highlight important details such as **source IP, destination IP, protocol type, and payload**.
3. **Opening .pcap Files**
   * Allow users to open and analyse .pcap files in a separate window.
4. **User-Friendly GUI**
   * Implement a **menu system** for navigation.
   * Include features like **Start/Stop Sniffing, Open PCAP File, About Section**.
   * Add an **Exit button** in the .pcap viewing window for usability.

**5. Future Aspects**

ScapyUI can be further improved by integrating the following enhancements:

1. **Filtering Mechanism**: Allow users to filter packets based on **IP address, protocol type, or port number**.
2. **Packet Editing** : Enable modification and replay of captured packets for penetration testing.
3. **Graphical Traffic Visualization**: Use Matplotlib or other visualization tools to represent network activity graphically.
4. **Automated Threat Detection**: Implement **basic intrusion detection** mechanisms to highlight suspicious traffic.
5. **Logging and Exporting Reports**: Save session details as text logs or CSV files for further forensic investigation.

**6. Conclusion**

ScapyUI is a **lightweight yet powerful network sniffer** designed to simplify packet analysis for security professionals, forensic analysts, and network engineers. By providing a **structured and user-friendly GUI**, it bridges the gap between command-line Scapy functionalities and more complex tools like Wireshark.

With its ability to **capture live traffic, save and open .pcap files, and categorize packet types**, ScapyUI serves as an efficient solution for network analysis. Future enhancements, such as **packet filtering, visualization, and automated threat detection**, will further elevate its capabilities, making it an essential tool for cybersecurity professionals.

**Developed by: Yash Rana**  
**Version: 1.0**