**National University Of Computer And Emerging Sciences Chiniot-Faisalabad Campus**

****

**CS3002 – Information Security**

**Project Proposal**

**Packet Sniffer**

**Submitted to: Dr. Muhammad Umar Aftab**

|  |  |
| --- | --- |
| **Name** | **Roll No** |
| Seemal Zia | 21F-9155 |
| Rimsha Sarfraz | 21F-9244 |

**Objective:**The objective of this project is to develop a (packet sniffer) a tool used in computer networks to capture and analyze network packets. The project aims to enhance the understanding of network traffic, network protocols, and information security concepts. By providing an interactive graphical user interface (GUI), users can easily specify a network interface, capture traffic, analyze captured packets, and save them for further examination.

**Features:**The packet sniffer will include the following features:

1. **Graphical User Interface (GUI)**:   
   The GUI allows the user to specify the network interface for packet capture, start and stop packet sniffing, and view the captured packets in real time. It will also include buttons to save captured packets to a file and clear the displayed information.
2. **Protocol Filtering**:   
   Users will be able to filter packets by protocol (e.g., TCP, UDP, HTTP), making it easier to focus on specific types of network traffic and understand different protocols in detail.
3. **Detailed Packet Analysis**:   
   The application will provide detailed information about each captured packet, including IP addresses, ports, MAC addresses, and other protocol-specific headers, allowing users to gain deeper insights into packet structures.
4. **Save and Load Captures**:   
   Captured packets can be saved in PCAP format, which can be analyzed later using tools like Wireshark. This feature allows flexibility for offline analysis and comparison.
5. **Network Traffic Visualization**:  
   A simple visualization feature will show the breakdown of packets by protocol type using charts. This helps users visualize the types of traffic present in the captured data.
6. **Alert System**:  
   A basic alert system will be implemented to notify users when a specific type of packet is detected (e.g., suspicious activity like repeated failed login attempts). This introduces the concept of simple intrusion detection.

# **Tools & Technologies**:

* **Pyshark**: A Python library for packet sniffing that provides access to network packet capture and detailed analysis.
* **Tkinter or PyQt**: Python libraries used to create a graphical user interface for packet sniffing tasks.
* **Matplotlib**: A library used to create visual representations of the captured packet data, making it easier to understand the distribution of traffic types.

**Project Scope and Benefits:**

This project is basically designed to provide hands on experience in the field of computer networking and information security. By building a packet sniffer, we will gain a comprehensive understanding of network packets, protocols, and data analysis. The inclusion of a GUI ensures that the tool is user friendly and accessible for beginners, while the protocol filtering, visualization, and alert features add depth for advanced users.

.

**Conclusion:**This project not only provides insights into how data flows through a network but also teaches essential concepts like packet analysis and network security. By using tools like Pyshark and Matplotlib, the project combines practical coding skills with real-world network analysis techniques. It will be a valuable addition focusing on the fundamentals of information security and networking.