Network Scanner GUI Documentation

1. Network Discovery (ARP Scanner)

The ARP scanner identifies active devices within a specified subnet by sending Address Resolution Protocol (ARP) requests to all possible IP addresses in the subnet. For each IP that responds, the tool captures the corresponding MAC address, as ARP is used to map IP addresses to hardware (MAC) addresses. This function is particularly useful for network reconnaissance, as it provides a quick overview of connected devices. The results, including detected IP and MAC addresses, are displayed and can be logged for further analysis.

Sends ARP requests to all IP addresses in a subnet to identify active devices. Captures and displays their corresponding IP and MAC addresses.

2. Packet Analysis

The packet analysis function captures and inspects network traffic for a specified IP address. Users can apply filters to focus on specific protocols such as TCP, UDP, or ICMP. For each packet, the tool displays essential details, including the source and destination IP addresses, source and destination ports, protocol type, and payload size. This functionality is crucial for identifying network anomalies, analyzing communications, and troubleshooting issues, providing insights into the behavior of devices on the network.

Captures network traffic for a specified IP and filters packets by protocol (TCP, UDP, ICMP). Displays source/destination IPs, ports, and protocol details.

3. Custom Packet Creation and Transmission

This function enables users to craft and transmit custom network packets to target devices. For example, users can generate ICMP echo requests (pings) to test connectivity or send TCP SYN packets to initiate a handshake with a specific port. Customizing packet headers allows for various use cases, such as network testing, performance assessment, or even stress testing. This feature empowers users to simulate different network scenarios, aiding in security assessments and network performance evaluations.

Allows users to create custom packets (e.g., ICMP, TCP SYN) with specific header fields. Sends packets to target IPs for network testing and analysis.

4. Traffic Monitoring and Logging

Traffic monitoring continuously captures network packets and logs them into a file for later analysis. Each log entry includes a timestamp, protocol type, source and destination IP addresses, and packet size. This function is essential for maintaining network visibility, detecting unusual traffic patterns, and investigating security incidents. By storing logs, users can perform offline analysis, correlate events, and maintain an audit trail of network activity over time.

Continuously captures and logs network packets with timestamps, protocol type, and packet size. Stores logs for offline analysis and security audits.

5. Network Performance Measurement

The network performance measurement function calculates key metrics like data rate, throughput, latency, and jitter. The data rate represents the amount of data transmitted over a given time, while throughput indicates the successful data delivery rate. Latency measures the time taken for data to travel from source to destination, and jitter reflects variations in latency. These metrics are logged into a file to help users evaluate network health, optimize performance, and identify potential bottlenecks or issues affecting the quality of service.

Calculates and logs network metrics like data rate, throughput, latency, and jitter. Helps assess network performance and identify bottlenecks or issues.