First! We need to open CMD run as administrator

The sniffer captures network traffic in real-time, processes it, and sends data to the web interface for analysis."

It Captures all IP traffic on your network, extracts important features like source/destination IPs, protocols, and packet sizes, Uses Scapy library for efficient packet processing, runs with administrator privileges for full network access.

"Now, let's move to the web interface. Open your browser and navigate to: <http://localhost/maltrail-php/public/index.php>

The dashboard shows:

- Real-time network traffic visualization

- Active connections

- Alert notifications

- Protocol distribution

I demonstrate the threat detection capabilities:

1. The system monitors for suspicious patterns

2. It checks for: - Abnormal packet sizes

- Unusual connection rates

- Suspicious protocols

- Known malicious Ips

Then all the log data is been save to log.json as database.