本课题主要包括：使用python从链路层到应用层进行流量分析并提取出重要信息，从流量中分析出隐藏的网络攻击和风险，最后将数据流量和网络威胁进行可视化。

系统大概流程：使网卡进入混杂模式进行流量监控，编写网络数据包解析器解析网络流量包，分析并且存储流量，分析网络中存在的安全隐患，最后使用可视化工具kibanna将其可视化。

该程序解决小型网络内实施网络安全监控需求，为小型网络安装昂贵的防火墙或者专业入侵检测工具给出了另一种解决方案。通过侦听网络流量包监控小型网络数据和用户上网行为，使用包过滤技术进行网络数据包的筛选，达到保护网络安全的目的。

该系统主要完成以下几个功能模块:

1. 主程序: 整个程序的入口点，用于控制整个程序。(预计300行)
2. 通用函数: 一些通用函数， 包括但不限异常错误处理函数，数据库处理函数等。(500行左右)
3. 流量分析模块: 进行流量分析，其中包含从链路层到应用层的数据结构的处理(200-300行左右)
4. :网络安全隐患分析模块：从抓取的数据包进行安全分析，找出其中的潜在威胁，如syn泛洪攻击， nmap网络扫描等。（500行左右)
5. 。数据可视化模块: 使用软件kibanna将分析出来的数据包进行可视化，是管理员能更加清楚的观察网络威胁。