题目：基于Linux平台的网络检测工具的实现

简介：伴随着互联网的高速发展，各种新的网络应用程序不断涌现，对计算机网络的监测就愈加显得重要，本系统在Linux平台上实现对本地网络的监测。系统通过将TCP/IP网络中传送的数据包头截获，它是网络分析、监测的基础，最终需要实现实时捕获流经本机的数据包，将网络数据包转换成可读格式，实时统计本机的流量以及网速，将以上这些信息显示图形界面上，方便用户更直观的获得信息。

**任务书**：

准备阶段：完成与基于Linux平台开发相关的理论、工具学习及资料查阅，完成英文翻译，做好开题准备；   
 需求设计：深入进行需求分析，进行详细系统设计；   
 搭建环境：安装相关工具，搭建开发环境，熟悉Linux相关库函数；  
 数据包捕获模块设计与实现：利用Linux库对流经本机的数据包进行捕获；  
 协议分析模块设计与实现：根据TCP/IP协议对捕获的数据包进行解码分析，准备中期检查；

网络流量模块设计与实现：统计网络流量，进行网速计算；  
中期检查反馈：根据中期检查结果，调整系统设计和功能；   
界面设计：根据系统功能进行界面设计，将监测结果以丰富的图形方式进行显示；   
 整体模块联调：将每部分模块进行联系组合，形成完整的模块；   
 测试及修改：测试系统的可用性、正确性和合理性，进行完善和修改；   
 撰写论文及准备验收：撰写系统相关文档和帮助文件，撰写论文，准备系统验收，准备答辩演示文档；   
 论文答辩：答辩、整理毕设归档资料。

**功能模块：**

Linux平台网络检测工具

数据采集模块

信息统计模块

流量绘制模块

异常检测模块

查询模块

．**数据采集模块**：完成网络接口数据的捕获、解析和显示，可以根据用户定义条件组合来进行捕获，如只监视采用TCP或UDP协议的数据包，也可以监视用户希望关注的相关IP地址的数据包，同时完成数据封包日志记录，提高了系统的灵活性。同时，在对数据包的解析过程中对一些常见入侵攻击特征进行判断，发出预警。该模块采用编写原始套接字开发。

**．信息统计模块**：完成统计功能，如统计IP要实现统计接收到的数据报数量、接收到的数据中协议出错的数量、正在请求传输的数量、路由表中可用路由数量、丢弃的数量、需要重组/成功重组的数量等，统计ICMP需要完成发送/接收的消息数量、满足超过TTL的数量、重定向数量、时间戳请求/应答数量等。采用IP助手函数完成。

**．流量绘制模块**：完成总流量、输入流量、输出流量、瞬时流量值、最高流量值的显示。采用访问注册表网络性能数据完成有关数据的获取，通过流量图显示。结果数值显示方式为柱状图。

．**异常检测模块**：对网络抓包头文件进行检测，看是否存在异常（病毒），若发现，弹出提示框。常见攻击分析功能:本设计中对部分常见的攻击行为进行了分析在解析过程中加入了常见攻击行为数据包的判断和报警比如Land、Ping of Death等攻击。

．**查询模块：**用户可进行简单查询，根据用户的某些要求，查询历史数据对某段时间内统计的总流量，平均流量进行数值显示。