南京邮电大学毕业设计（论文）指导记录

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 题目 | Linux平台下网络协议分析工具的设计与实现 | | | | |
| 学生姓名 | 徐秋硕 | 班级学号 | B13070135 | 专业 | 网络工程 |
| 指导教师姓名 | 李养群 | | | 指导教师职称 | 讲师 |
| 日 期 | 毕业设计（论文）进度 | 毕业设计（论文）过程中遇到的问题 | | 下一步工作计划 | 指导教师审核意见 |
| 2017-02-23 | 资料查阅和相关技术调研基本完成，根据导师推荐书籍，例如网络协议分析工具的设计与实现等，对于课题有明确的认识。需求分析，概要设计大概已完成。 | Linux平台技术的学习有所难度，在导师沟通指导下顺利抓起；底层网络协议的重温还是具有相当的难度的。 | | 根据实际工作中掌握的知识，配合此次项目的实际需要，进一步学习socket套接字的应用开发。抓住导师以及身边的同学这些资源，在半个月之内开发出网络数据包捕捉工具。 | 同意 |
| 2017-03-14 | 目前大概设计工作和需求已经完成了，经过导师的指导，并研读了相关著作，网络协议分析，捕获和监听网络数据包并进行分析的方法大概已经成型。 | 协议分析工具制作概念模糊，是否像wireshark的功能需求一样，经过思考与求助，大概功能设计已完成，无需wireshark那样的全面，协议分析目的才是关键。协议分析书籍还需要去仔细研究，抓包分析工具的制作还有相当大的难度。 | | 学习如何利用Socket原始套接字捕获数据，即java的深入学习和开发使用，针对相应功能需求，难度攻克，针对性的学习理解并应用，争取尽快将抓包分析工具制作出来。 | 同意 |
| 2017-04-05 | 根据前期的准备工作，进行概要设计，以及技术方案确定，下载并熟悉使用相关辅助工具。  确定了网络数据包协议分析工具的层次并进行设计：1.数据输入模块，该模块主要功能是接收用户输入用于捕获数据包的信息；2.数据捕获模块，该模块的主要功能是捕获流经本地网卡的所有数据； 3.规则匹配模椋该模块的主要功能是根据用户的需求对需要捕获的数据包进行过滤设置，因为不是所有经过本地网卡的数据报都对我们分析网络有用；4.数据处理模块，该模块的主要功能是对捕获的数据进行分析显示处理；5.协议分析模块，该模块的主要功能是对捕获的数据包进行协议分析；6.显示模块，该模块的主要功能是将分析的结果显示给用户，对数据包进行协议分析后要把结果 显示给用户本程序才结束，且根据要求，本次是需要实现图形化界面显示。 | 显示模块原计划选用的是Delphi技术实现，经过导师提示，这已经是过时的技术，随后改用ＱＴ应用框架， 它包括一个直观的API和一个丰富的类库，以及用于GUI开发和国际化的集成工具，另外它支持java和C++开发。 | | 根据初步设计文档，进行网络协议分析工具的设计与开发实现，在Linux平台下，利用socket套接字捕获数据，并利用图形化界面显示分析结果。 | 同意 |
| 2017-04-21 | 在Linux平台下，利用socket套接字捕获数据，深入研究课题的设计内容，进行各个模块的功能设计开发，优化界面显示结果，界面开发选用QT，力争图形界面做出想要的效果。 | 协议分析模块遇到瓶颈，该模块的主要功能是对捕获的数据包进行协议分析，把数据包捕获下来后，我们需要对其分析才能知道网络中存在的安全问题，该模块主要是对TCP/IP各层的协议进行分析。该方面的知识储备没有预期的充足，因此还要进一步加强学习研究。 | | 对各个模块（数据输入模块，规则匹配模块，数据处理模块，协议分析模块，显示模块）的进行整合，分析，调试以及修改，达到预期的效果。 | 同意 |
| 2017-05-08 | 本阶段主要进行协议分析模块的设计，该模块的主要功能是对捕获的数据包进行协议分析。把数据包捕获下来后，我们需要对其分析才能知道网络中存在的安全问题，该模块主要是对TCP/IP各层的协议进行分析。同时协议分析系统的框架已经基本完成，等待每个模块的最终润色以及模块完成后整体功能的调试分析。 | 对协议安全隐患的产生途径不太明确，经过导师和同学的帮助，了解了其中的原理：  TCP使用三次握手时，攻击者冒充发送方发送ack包，攻击者便达到了破坏连接的作用，若攻击者再趁机插入有害数据包，则后果更严重；    IP层的安全问题是IP地址假冒；    ICMP存在的安全隐患是攻击者可利用ICMP重定向报文破坏路由，可利用不可达报文对某用户节点发起拒绝服务攻击。 | | 对各个模块进行补充整合，分析，调试以及修改，达到预期整体的效果，对TCP/IP协议数据包能够进行有效的分析，并进行图形化界面显示，也就是最重要的一步，为最终的设计完成打下最坚实的基础。并进入整理总结阶段，将开发成果运行起来。 | 同意 |
| 2017-05-22 | 论文初稿已经完成，总共分六个章节：  第一章绪论  第二章系统相关技术 第三章系统功能需求分析  第四章系统设计与实现  第五章测试和结果分析  第六章总结与展望  目前已经将初稿发给导师，进行进一步的指导，系统实物也已经完成，论文与实物还需要打磨润色，进一步的加工才能完成。 | 论文具体格式不是很清楚，后来得到相关文件的统一格式，还有一些论文中的相关资料查重时可能重合率有点高，需要将相关技术进行改进。 | | 对论文进行进一步打磨，再进行查重，降低重合率，最终准备PPT进行答辩。 | 同意 |