实验 2 逆向工程套接字编程实验

2.1 实验目的

理解协议的逆向分析方法并掌握客户端套接字编程。

2.2 实验说明

在本实验中，我们将利用上一个实验中掌握的 Wireshark 数据包嗅探技术来逆向分析一个协议，并使用套接字编程技术重新实现该协议的客户端。

同学们需要重新实现的是一个天气查询系统，我们提供了它的 windows 和 Linux 客户端程序，要注意的是，对于 Linux 客户端，在下载之后你需要将它的文件权限改为可执行（执行命令：`chmod a+x program_name`）。

2.3 实验内容

1. 你的任务是在运行该程序的同时运行 Wireshark，捕获在你的电脑和该客户端所连接服务器之间交换的报文。在运行该客户端时，你最好关闭电脑中运行的其他网络程序，以方便你的观察。你应该捕获针对每一个选项的报文，以便对协议有一个完整的了解。
2. 一旦你认为已完全理解了该协议，你就可以开始用 C 语言在 Linux 系统中编写自己的客户端程序。你的客户端程序应完整实现原客户端所有内容，特别需注意各种边界情况的处理。
3. 原客户端在和服务器通信的过程中，会包含两个隐藏的 Flag，你能发现吗？

2.4 实验提交

1. 提交的作业应包括以下内容，请将这些文件打包压缩后提交。实验报告（PDF 文件）和打包压缩文件（rar 文件或 zip 文件）的文件名前缀统一为：学号_lab02：
   (1) 进行协议逆向分析所使用的 Wireshark dump 文件；
   (2) 客户端程序源代码软件包（包括 readme 文件、Makefile 文件和源代码文件），其中 Makefile 文件用于编译你的程序，readme 文件应简要描述你的程序作用和运行程

序的方法；

(3) 实验报告。

2. 程序应遵循良好的编程规范，需添加注释以提高代码的可读性。
3. 如果你在实验报告中引用了其他资料，必须在报告中注明。
4. 实验报告中应包括的内容如下所示：

实验目的	
实验内容	说明：描述程序的设计思路和实现方法，包括实验的设计流程图/关键代码等。
实验结果	说明：实现了哪些功能，并给出主要功能的实现截图。
实验中遇到的问题及解决方案	说明：没有解决的问题也可以写在这里。
实验的启示/意见和建议	
附：本次实验你总共用了多长时间？包括学习时间、编写代码时间和测试时间。（仅做统计用，时间长短不影响本次实验的成绩。）	