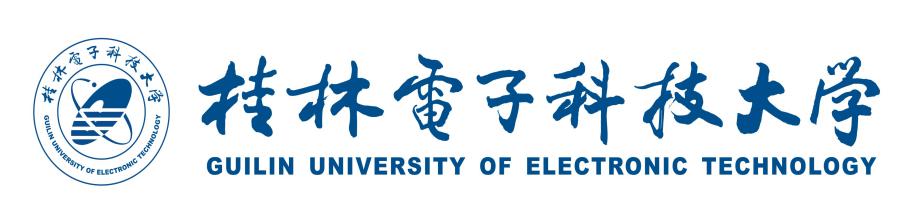
编号：

****

毕业设计说明书

题 目： 网络扫描软件

学 院： 计算机与信息安全学院

专 业： 计算机科学与技术

学生姓名： 邓克厘

学 号： 1400310310

指导教师： 韦必忠

职 称： 副教授

题目类型：🞎理论研究 🞎实验研究 🞎工程设计 🞎工程技术研究 🗹软件开发

2019年5月15日

摘 要

时至今日，互联网已经深入人们日常生活的方方面面，大家在网上浏览新闻，购物，办公，支付宝的创立，标志着网络进一步融入人们生活当中。享受着互联网便利的同时，一些安全问题开始逐渐尖锐起来。2017年4月，优酷一千万条用户账户信息在暗网出售；同年三月，58同城曝重大个人信息泄密，700元可看所有人简历；2018年8月，温州乐清滴滴顺风车命案引发对私隐的警醒；2017年5月12日，“WannaCry”（想哭）比特币勒索病毒在全球范围内爆发，本次事件波及150多个国家和地区、10多万的组织和机构以及30多万网民，损失总计高达500多亿人民币；网络安全形势不容乐观。

习近平总书记在全国网络安全和信息化工作会议上发表讲话时曾说，没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障。2016年，我国出台《网络安全法》，进一步整治网络环境，网络安全重视程度达到空前高度，网络安全相关的软件应运而生。

网络扫描软件就是网络安全软件的一种，它针对本地或远程计算机系统进行扫描，了解系统的端口开放情况，服务开放情况，以及运行该服务的软件及其版本，并根据以上信息，判断系统是否存在漏洞及安全隐患等，为网络管理员管理系统提供了有力的帮助，为防止网络攻击提供了一道坚实的屏障。本软件采用B/S架构，前端为交互界面，后端处理数据，完成核心功能。用户能采用本软件扫描本机系统，完成系统脆弱性检查，同时能获得针对性的改进建议，完善系统的安全防护。

关键词：B/S;网络扫描；网络安全

**Abstract**

Today, the Internet has penetrated into every aspect of people's daily life. When we browse news, shop and work on the Internet, the creation of Alipay symbolizes the further integration of the Internet into people's lives. While enjoying the convenience of the Internet, some security issues are becoming increasingly acute. In April 2017, Youku sold 10 million user account information on the secret internet; in March of the same year, 58 people in the same city disclosed significant personal information leaks, 700 yuan can see everyone's resume; in August 2018, Wenzhou Yueqing drip-drip homicide case triggered a wake-up to privacy; on May 12, 2017, "WannaCry" (Wanna Cry) Bitcoin extortion virus broke out worldwide, the incident affected more than 150 countries. Home and region, more than 100,000 organizations and institutions and more than 300,000 netizens have lost more than 50 billion yuan in total. The situation of network security is not optimistic.

In his speech at the National Conference on network security and information technology, General Secretary Xi Jinping said that without network security, there would be no national security, no stable economic and social operation, and the interests of the broad masses of the people would be difficult to guarantee. In 2016, China promulgated the "Network Security Law" to further rectify the network environment. The importance of network security has reached an unprecedented level. Software related to network security emerged at the historic moment.

Network scanning software is a kind of network security software. It scans local or remote computer systems to understand the opening of the system's ports, the opening of the service, and the software and its version running the service. Based on the above information, it judges whether there are loopholes and security risks in the system. It provides a powerful help for the network administrator management system and prevents them. Stopping network attacks provides a solid barrier. The software adopts B/S architecture, the front end is an interactive interface, the back end processes data, and completes the core functions. Users can use this software to scan the local system, complete the system vulnerability checking, at the same time can get targeted improvement suggestions, improve the security of the system.

**Key words** ：B/S;VUE;HTTP;MVVM;Online Student Work

目 录

[引言 1](#_Toc515384914)

[1 课题背景及调研情况 2](#_Toc515384915)

[1.1 研究背景及意义 2](#_Toc515384916)

[1.2 研究目的 2](#_Toc515384917)

[1.3 本文主要工作 2](#_Toc515384918)

[1.4 论文的组织 2](#_Toc515384919)

[2 网上作业管理系统开发相关技术 3](#_Toc515384920)

[2.1 前端技术 3](#_Toc515384921)

[2.2 后端技术 4](#_Toc515384922)

[3 可行性与需求分析 5](#_Toc515384923)

[3.1 可行性分析 5](#_Toc515384924)

[3.2 需求分析 5](#_Toc515384925)

[3.2.1总体需求 5](#_Toc515384926)

[3.2.2后端总体模块需求分析 5](#_Toc515384927)

[3.2.3前端总体功能模块 6](#_Toc515384928)

[3.2.4基本用户管理模块 6](#_Toc515384929)

[3.2.5学生的课程和作业管理模块 7](#_Toc515384930)

[3.2.6教师的课程和作业管理模块 7](#_Toc515384931)

[4 系统设计 9](#_Toc515384932)

[4.1 主要页面的设计 9](#_Toc515384933)

[4.2 数据库结构设计 10](#_Toc515384934)

[4.2.1数据库设计概述 10](#_Toc515384935)

[4.2.2系统总体数据关系 10](#_Toc515384936)

[4.2.3数据库表结构的设计 11](#_Toc515384937)

[5 系统实现与编码 15](#_Toc515384938)

[5.1 系统主要功能实现 15](#_Toc515384939)

[5.1.1基本用户管理功能实现 15](#_Toc515384940)

[5.1.2教师课程管理功能实现 17](#_Toc515384941)

[5.1.3教师作业管理功能实现 19](#_Toc515384942)

[5.1.4学生功能实现 22](#_Toc515384943)

[5.1.4管理员审核功能实现 24](#_Toc515384944)

[5.2 主要页面和所用到的restful api 25](#_Toc515384945)

[5.2.1教师主要界面 25](#_Toc515384946)

[5.2.2学生主要界面 29](#_Toc515384947)

[5.2.3管理员界面 32](#_Toc515384948)

[6 系统测试 33](#_Toc515384949)

[6.1 注册和登陆功能的测试 33](#_Toc515384950)

[6.2 教师的课程管理功能的测试 33](#_Toc515384951)

[6.3 教师的作业管理功能的测试 34](#_Toc515384952)

[6.4 学生功能的测试 35](#_Toc515384953)

[6.5 管理员审核功能的测试 36](#_Toc515384954)

[7 结束语 38](#_Toc515384955)

[7.1 系统的主要功能 38](#_Toc515384956)

[7.2 系统不足之处 38](#_Toc515384957)

[谢 辞 39](#_Toc515384958)

[参考文献 40](#_Toc515384959)

[附 录 41](#_Toc515384960)

# 引言

网络安全是指网络中的硬件系统、软件系统及其系统中涉及的数据因受到预设的保护， 而可以连续、可靠、正常地运行，并不因偶然事故或者恶意处理而遭受破坏、非法更改、信息泄漏。目前世界网络安全形势日益严峻，国家对网络安全空前重视。在这样的背景下，网络扫描软件就显得尤为重要了。它能扫描出系统的基本安全情况，为管理员维护系统安全提供给了必要参考信息。

论文设计实现一个基于B/S架构的在线网络扫描软件，分为扫描与评估两大模块，扫描模块负责实现端口及服务的探测功能，评估模块只针对扫描结果，进行一系列模拟攻击测试，以检测处系统的脆弱性情况。本系统选取轻量级的Flask框架进行web开发。Flask框架具有功能丰富，轻量易用等优点，适合本系统的开发。前端采用html/css/js等动态网页技术构建友好美观的操作界面；后端采用nmap、scapy等库完成部分扫描模块，采用多线程与网络编程等技术完成评估块。Nmap库能提供一些基础端口扫描功能，具有扫描速度快，扫描信息准确等优点。前后端采用ajax异步交互，交互格式采用json，ajax广泛用于web开发中，是实现动态网页的基础。

本文广泛调研网络扫描技术，采用了先进的syn半连接扫描技术，扫描准确快速。采取B/S模型，前后分离，界面在浏览器，核心实现在服务器，具有易维护，易使用等优点。本文针对前后两端以及扫描模块与评估模块给出了出详细设计和数据结构，设计流程和系统可用性及稳定性的测试等，在本文中选取主要实现部分进行了说明。

# 1 课题背景及调研情况

1.1 研究背景及意义

网络与生活关系日益紧密，移动支付更是基本取代了纸币，成为人们消费主要方式，因词，对网络安全的要求空前强烈。一款优秀网络扫描软件能直接帮助网络管理员了解系统基本安全情况，让网络管理员能更好的配置系统，以达到系统的安全。

1.2 研究目的

主要是为了检测系统的脆弱性，评估系统是否可被攻击，同时给出一些针对性改进意见，以帮助管理员更好、更安全的管理系统，避免因为系统不安全而带来经济损失。

1.3 本文主要工作

1. 阐明网络扫描软件的开发背景和意义。
2. 整合开发中用到的设计思想技术以及相关技术，记录整个系统的开发过程，以及解决困难的思路与体会。
3. 分析本软件的需求、设计过程、开发过程，总结其中的技术精髓。

（4） 统计软件的测试结果，测试系统的稳定性与效率。

1.4 可行性分析

（1）技术可行性分析：本软件主要涉及网络编程、多线程编程、web开发以及网络安全基本技术，而大学的一些课程：《计算机网络》、《程序设计与问题求解》以及《网站规划与设计》等课程解决了上述技术的理论基础，而网络安全相关技术容易从搜索引擎获取，故而本软件在技术上可行。

（2）法律可行性分析：本软件属于自主开发，不存在抄袭等问题，网络安全法中有相应规定，未经授权的渗透测试属于非法行为，然而软件本身是违法的，因此本软件不存在法律问题，法律上是可行的。同时，本软件所采用的的库均属开源库，本软件也将遵循开源条例进行开源。

（3）需求可行性分析：网络安全形势严峻，用户信息泄露、电信诈骗以及盗刷盗用等黑客事件层出不穷，网络扫描软件应运而生，成为维护网络安全的一道坚实屏障，各互联网公司均有不同程度的安全需求，本软件可帮助公司的网络管理员管理系统与维护安全，同时个人用户也可使用本软件，减少系统被攻击的风险。综上，本软件在需求上是可行的。

1.5 论文的组织

本文总共分为七章，各章节的主要内容如下：

第一章：主要说明网络扫描软件的需求背景及调研情况。主要介绍了研究的背景及意义、研究目的、可行性分析和论文等主要工作。

第二章：介绍完成网络扫描软件用到的相关技术。

第三章：对网络扫描软件进行需求分析。

第四章：描述软件实现的具体开发情况，介绍系统的主要功能。

第五章：测试软件功能与效率，包括扫描测试及评估测试，分析测试结果

第六章：总结收获以及对软件的评价与展望。

# 2 开发技术

2.1 前端技术

2.1.1 HTML和CSS

HTML指的是超文本标记语言 (Hyper Text Markup Language)，它是一种构建网页的基础技术，HTML语言形式为尖括号包围着元素名字，它支持插入图像，音频等。HTML代码经由浏览器渲染后变成我们所看到的网页，开发环境极为简易，只需一个文本编辑器即可，它与css\js统称为前端三剑客，是网页开发的基石。

Css(英文全称：Cascading Style Sheets)中文名层叠样式表，用来静态的修饰网页，设置网页的样式，颜色，字体等。Web网页的内容绝大多数都是文字，Css可以用来修饰文字的大小，字体等使网页文字更加亲切美观，同时它还能控制网页给内容的排版，使网页错落有致，更加得体优雅。

2.1.2 JavaScript和AJAX

Javascript简称js，是一种用于网页的脚本编程语言，它与大名鼎鼎的Java毫无关系，当初其发明人为了推广而去蹭了一波Java的热度。Js能直接在浏览器中执行，支持面向对象编程，命令式编程与函数式编程。Js能直接操作浏览器元素，使得修改网页变得异常轻松，它还能制作网页许多动态效果，是现代动态网页技术的基石。

Ajax（Asynchronous JavaScript + XML）是一种设计模式。过去的网页采用的是静态技术，即使请求的网页只要细微的差距仍然需要重新加载完整的网页，ajax技术的就是为了解决这一尴尬的局面，它本质是js，但是它允许网页进行异步数据交互，即允许网页只更新部分内容，主要通过xmlhttprequest对象完成主要功能。

2.2 后端框架

后端技术主要采用了flask框架技术，flask是一个轻量级的满足wsgi规范的web开发框架，其中jinja2引擎可以渲染html模板，完成前后端分离，使前端人员专心于精美界面的设计，后端人员能专注于数据与逻辑而不必操心于前端的代码。Flask基于wsgi规范，进行更高层的抽象，一个URL一个处理函数的模式，极大的提高了web开发效率，简单易用而又不失强悍功能，是本系统主要后端技术。

2.3 开源库

2.3.1 nmap与python-nmap

nmap是一款优秀的开源端口扫描软件，python-nmap模块提供了python与nmap交互的开发接口。Nmap能进行端口扫描，服务探测以及版本探测，扫描准确稳定，但是速度稍慢，本系统采用它进行完全系统的扫描，而快速扫描时采取其他技术。Nmap模块是端口扫描与服务发现的中坚模块。

2.3.2 scapy

Scapy是一个出色的数据包处理库，它能够方便的构造和发送数据包，同时它还能嗅探网卡上的数据包，支持自定义筛选条件，并且解析成比较友好的格式。本系统数据包的处理基本使用scapy完成。Scapy模块是端口扫描与服务发现的重要模块。

2.3.3 request

request是一个优秀的http请求处理库，request可以很方便的处理http数据包。它主要有get和post两个函数，分别处理http的get和post请求，通过两个函数的调用情况可判断目标端口是否开放web服务，request模块是进行web服务发现的关键模块。

2.3.4 FTP

FTP模块是一款很不错的FTP服务处理相关的模块，他可以完成FTP连接以及基本的FTP功能，本软件将使用FTP模块进行暴力破解测试。

2.3.5 paramiko

Paramiko模块用于ssh服务，可以完成ssh服务的基本功能，这里我们只需要它的连接功能即可，将在ssh爆破测试中用到。

2.4 端口扫描技术

端口扫描技术种类繁多，主流的有以下几种：

2.4.1完全连接扫描

一次完整的tcp连接建立需要请过三个阶段，首先，客户端向服务端对应端口发送syn包，清酒建立连接；然后，服务端对应端口收到客户端的syn包后，回复一个syn ack包进行确认；最后，客户端回复一个ack包确认，至此，连接已建立好。完全连接扫描即与服务端对应端口建立tcp连接，若能够建立连接则改端口开放，否则不开放或者被防火墙过滤

2.4.2 syn半连接扫描

所谓syn半连接扫描，就是在握手的第一阶段，正常发送syn包，然后嗅探服务器对应端口的反应，倘若发送过来的是一个正常的sn ack包，则说明端口开放，返回一个rst包关闭连接；倘若收到的是一个rst包，则说明对应端口关闭，什么也不用做；倘若服务器对应端口无反应，则说明发送的syn包被服务器防火墙过滤。Syn扫描相对于全连接扫描，具有速度快，占用资源少的优点，准确性也比较高，因此，本系统采用syn扫描进行端口扫描。

2.5 服务发现技术

2.5.1 ftp服务发现

ftp服务发现通过与指定端口建立tcp连接，客户端发送ftp命令并监听服务端回应，若服务端发回符合ftp协议的数据时，认为端口存在ftp服务，否则没哟ftp服务，遍历所有开放的tcp端口，即可测出ftp服务开放情况。

2.5.2 ssh服务发现

ssh服务发现通过与指定端口建立tcp连接，并且侦听服务端回应，通常若开放有ssh服务的话，服务端会返回一个banner，上面会说明ssh服务的版本，运行的软件等等欢迎信息，此时用正则表达式匹配即可判断是否有ssh服务。但是banner可以被人为修改，所以这种判断并不准确，此时需要调用nmap库的相应功能，发送一些特定的数据包并且监听服务器回应来综合判定是否有ssh服务。

2.5.3 web服务发现

Web服务发现通过request模块的get函数判断，get函数接收一个url作为参数，将目标IP与端口构造成url，传入get函数。即可通过调用request.get函数的反应得出是否具有web服务，request.get()函数不报错则存在web服务，否则没有web服务。

2.6 网络攻击技术

网络攻击（Cyberattack，也译为赛博攻击）是指针对计算机信息系统、基础设施、计算机网络或个人计算机设备的，任何类型的进攻动作，网络攻击种类繁多，不胜枚举，本系统将采用两种比较具有通用性的攻击技术去测试系统安全性。

2.5.1 爆破测试

爆破攻击又称蛮力攻击，通过对用户名与口令进行蛮力穷举，非法登录主机或者一些服务，如ftp或者ssh等。爆破攻击虽然原理简单，但是一直是危害非常大的漏洞之一，常年位列owasp十大漏洞前三。通常，能进行100次以上的口令尝试而没有任何防止措施的服务，视为具有爆破漏洞，若能较快爆破成功，则同时还存在弱口令漏洞。本软件将会对ftp服务和ssh服务进行爆破测试。

2.5.2 dos攻击

Dos（拒绝服务）攻击是指，通过对某服务进行多个请求，耗尽服务器带宽或者资源。Dos攻击有多种手法，本软件将采用syn-flooding手法进行dos攻击测试。当服务器接收到syn包时，进入半连接状态，会在协议栈种分配出空间，维护这个半连接，同时回复一个syn ack到客户端，倘若客户端一直没回应，则服务端会不停重发syn ack包并且维护半连接直到超时，而系统能够维护的半连接数是一定的。因此，只要在超时的这段时间内，有大量的syn包发到服务端，服务端就会因为维护大量的半连接而耗尽资源，而客户端相对于服务端损耗的资源可忽略不计。

# 3 需求分析

# 3.1输入输出需求

软件需要对给定的IP地址和端口进行处理，输出端口开放信息，端口上的服务信息，以及运行服务的软件信息，而后，需要对主机进行安全评估，输出主机的基本安全情况，一些村子的漏洞，根据主机安全信息，进一步输出一些安全加固建议。

3.2后端需求

后端负责接收前端传来的数据，进行加工处理，而后传回前端。本软件后端设计如下：

（1）扫描模块：接收前端传来的IP与端口信息，对主机进行扫描，得出给定端口的开放信息，端口上运行的服务信息，运行服务的软件信息以及软件的版本信息，并返回前端。

（2）评估模块：针对扫描得出的信息，针对ftp与ssh服务进行爆破测试，评估这些服务是否存在可爆破以及弱密码的漏洞；针对web或其他tcp端口进行dos测试，评估出主机是否可进行dos攻击。根据上述主机安全情况，给出加固建议，返回前端。

后端模块如图3.1所示：

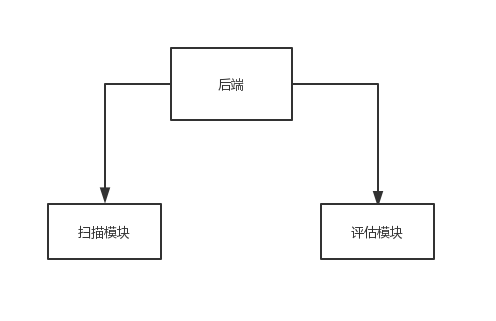


图 3.1后端模块图

（3）统筹模块：统筹模块负责将个功能模块与前端界面有机整合起来，具体来说，接收前端请求，条用扫描或评估等功能模块处理数据，最后将数据返回前端，是前后端的桥梁。

3.3前端界面需求

前端通过ajax与json与后端交互，将IP与端口信息传到后端并接受后端处理后的信息，将信息人性化、整齐和优雅地展示出来。

3.4测试环境需求

本次毕设除了实现软件之外，为了演示软件的功能，需要搭建测试环境，测试环境为端口扫描，服务发现，模拟攻击等功能提供一个靶场的功能，需要一个稳定的操作系统，并在系统上搭建一ftp、ssh以及web等服务以供测试。

3.5非功能需求

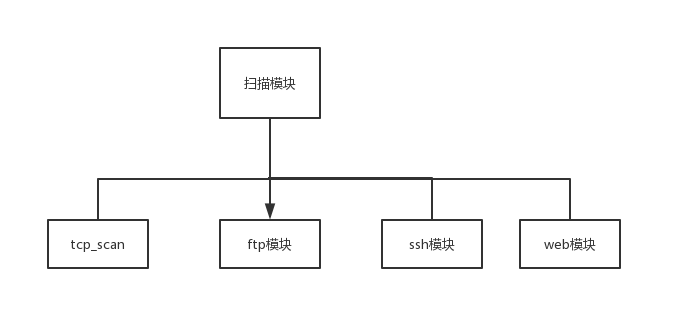
软件除了实现必备的功能之外，还必须稳定可靠，能处理各种数据输入，非法的输入要有提示信息，合法的要能正确处理，运行稳定正常，不会异常崩溃；同时，在兼顾稳定的基础上运行速度不能太慢，由于软件直接与人交互，而人的等待上限通常在一两分钟之内，超出了并会严重降低用户体验，因此本软件对性能眼球颇高。

# 4 系统设计

4.1 界面模块

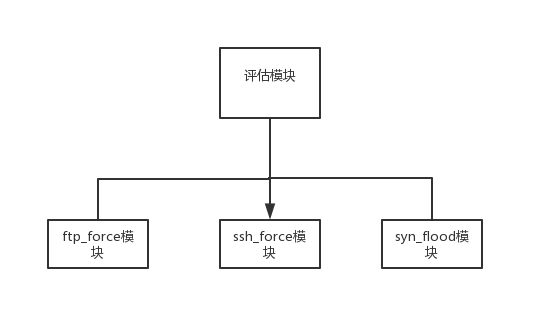
界面模块实现了人机交互界面，提供一些输入框与按钮供用户提交信息，并且合理设置一些空间来展示处理结果。

4.2 扫描模块

扫描模块实现了软件的全部扫描相关的功能，包括端口扫描，服务扫描，服务软件探测与版本探测等。扫描模块下共有：tcp\_scan模块、ftp模块、web模块、ssh模块。如下图所示：

Tcp\_scan模块完成tcp端口开放情况扫描，ftp模块完成ftp服务发现扫描，ssh模块完成ssh服务发现扫描，web模块完成web服务发现扫描。

4.3 评估模块

评估模块针对扫描出的信息，进行ftp爆破测试，ssh爆破测试，syn\_flood测试，从而检测出系统是否具有一些漏洞，安全情况如何，主要分为以下几个模块：ftp\_force模块，ssh\_force模块，syn\_flood模块，如图：

ftp\_force模块完成ftp服务的爆破测试，ssh\_force完成ssh服务的爆破测试,syn\_flood模块完成对主机dos攻击测试。

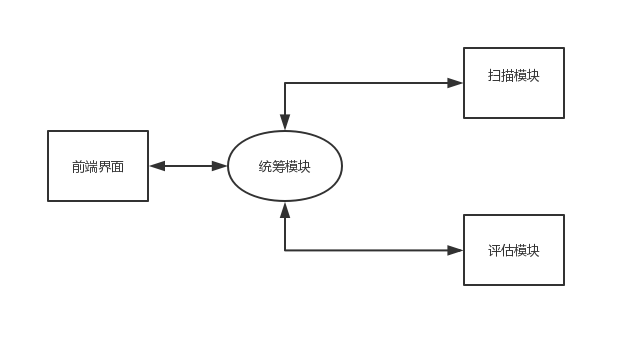
4.4 统筹模块

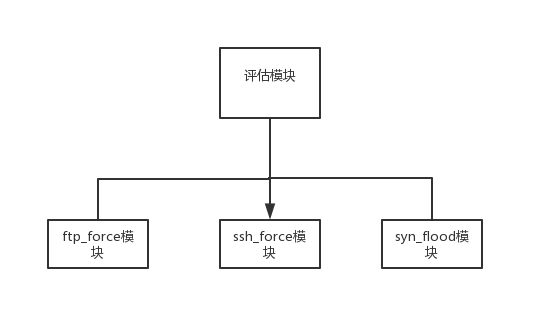
统筹模块充当界面与功能模块交互的桥梁，负责接收前端数据，调用相关功能模块处理，而后将处理后的数据返回前端。

4.5 测试环境

测试环境将设于虚拟机中，由一个操作系统充当，并在操作系统上搭建一些服务

4.6 综合设计

系统各个子模块的设计如上所述，他们关系如图：



# 4 系统实现

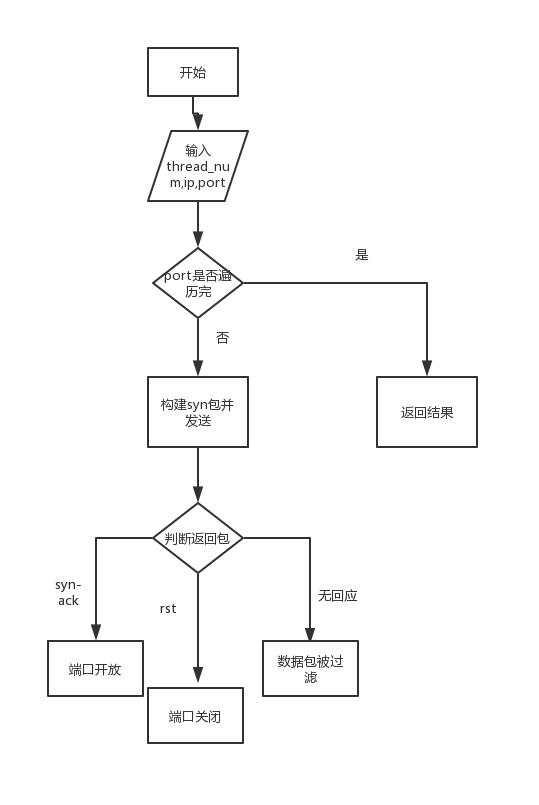
4.1 概述

用户面对前端界面，输入IP与端口信息，前端通过ajax请求将数据发回后端，同时等待后端返回数据，后端统筹模块接收到数据，调用对应功能模块（扫描模块或者评估模块）进行处理，处理好后由统筹模块返回数据。

4.2 端口扫描模块

Tcp端口扫描主要通过tcp\_scan模块实现，该模块需要的输入为：thread\_num(线程数量)，ip（目标IP），port(待扫描的所有端口)。该模块调用scapy模块的TCP（）以及IP（）构造一个具有目标IP和目标端口的数据包，将标志位置为’S’，然后调用scapy模块的Raw（）函数将数据包校验和计算好，调用scapy模块的sr1模块发送数据包并接受一个回应，对回应进行判断即可得出扫描结果：无回应说明数据包被防火墙过滤，无法判断结果；回应为syn ack包，即端口开放；回应为rst则端口关闭。

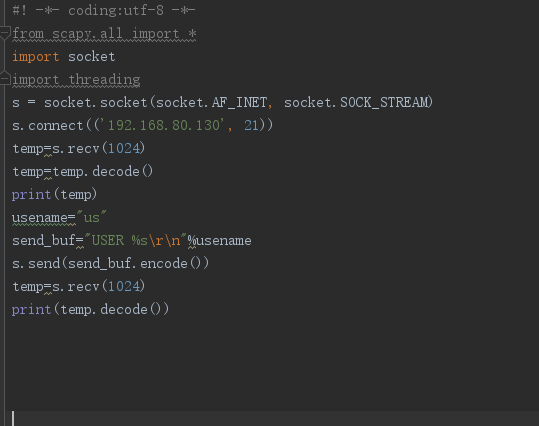
功能运行流程如图：



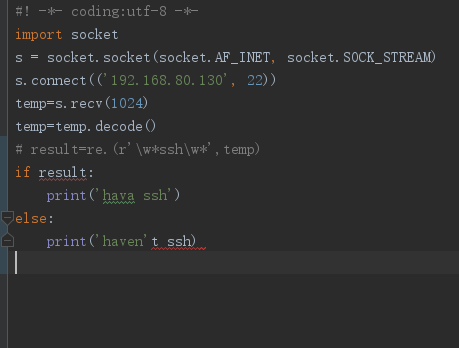
4.3服务发现

5.3.1 ftp服务发现

ftp服务发现功能封装于ftp模块中，该模块需要的输入参数为：ip(目标IP)，port(要检测的所有端口)。ftp模块调用python提供的socket接口，建立socket连接，通过连接发送符合ftp消息格式的消息，即”USER xxx\r\n”，发送后监听连接的回复消息，倘若符合ftp协议格式，则存在ftp服务，否则不存在。关键代码如下：



4.3.2 ssh服务发现

ssh服务封装于ssh模块，该模块需要的输入参数为：ip(目标IP)，port(要检测的所有端口)。通过与目标端口建立连接并且接收服务端信息，通过正则表达式进行匹配，看看banner是否存在ssh等关键字，从而判断是否存在ssh服务。关键代码如下：

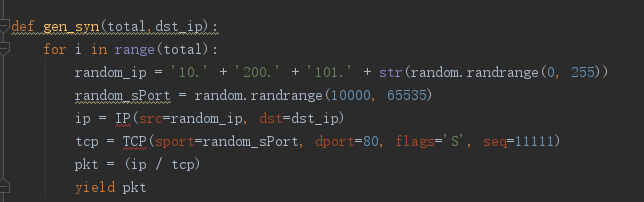
4.3.3 web服务发现

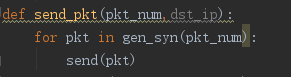
Web服务发现模块主要借助request模块完成，web模块接收输入参数为：ip(目标IP)，port(要检测的所有端口)，通过ip与端口构造一个url，作为参数传入request.get函数，根据get函数的返回信息即可判断是否具有web服务，若调用函数正常，则说明存在web服务，倘若函数调用抛出异常，说明不存在web服务，关键代码如下：

4.4 模拟攻击

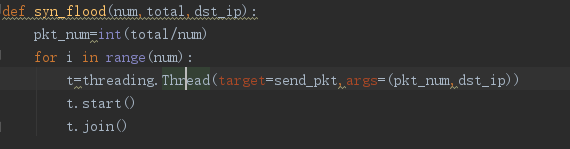
4.4.1 syn\_flood攻击

Syn\_flood攻击通过三个函数实现：gen\_syn(toal，dst\_ip)，该函数是一个生成器，每一次yield产生一个随机源IP、随机源端口、随机目的端口和指定IP的syn包,参数分别为生成的最大数据包数量与给定的目的IP；send\_pkt(ptk\_num,dst\_ip),该函数负责发送数据包，第一个参数指明每个进程发送的数据包数量，第二个参数作为第一个函数的参数（第二个函数需要调用第一个函数）；syn\_flood（num，total,dst\_ip）,该函数负责完成syn\_flood攻击，num为进程数量，其他参数意义同上所述，各函数具体实现如下：

gen\_syn(toal，dst\_ip)：

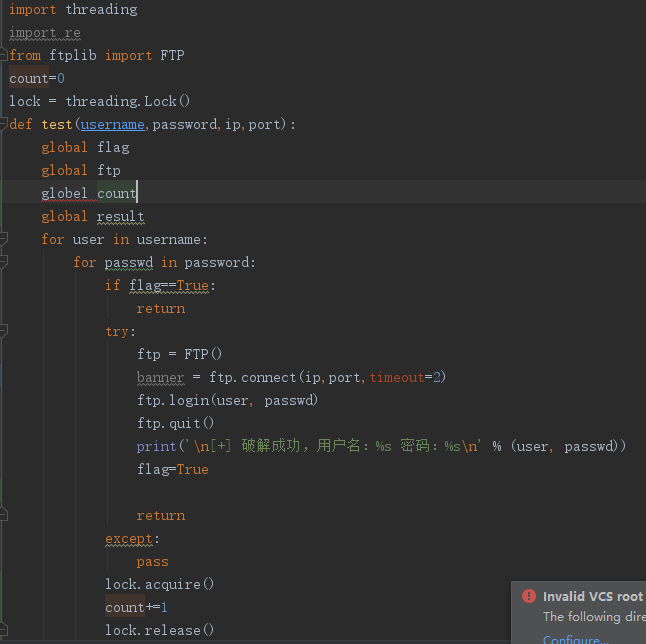
send\_pkt(pkt\_num,dst\_ip):

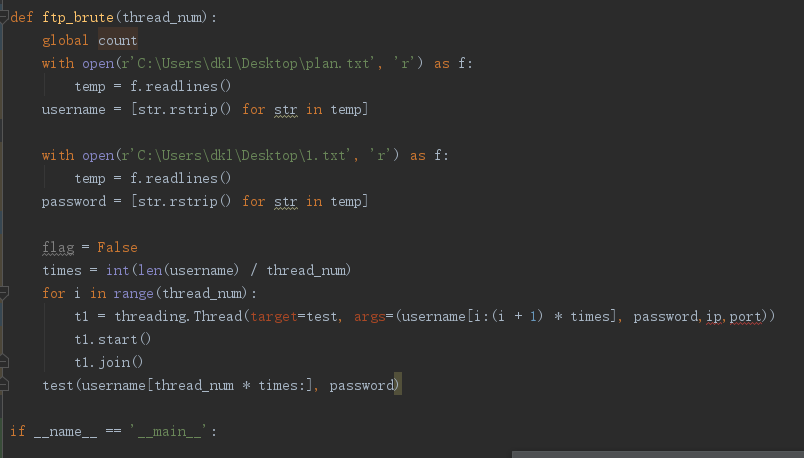
syn\_flood(num,total,dst\_ip)：

用total除以num得出每个进程需要发送的数据包数量，剩下的就是调用前面的函数即可：

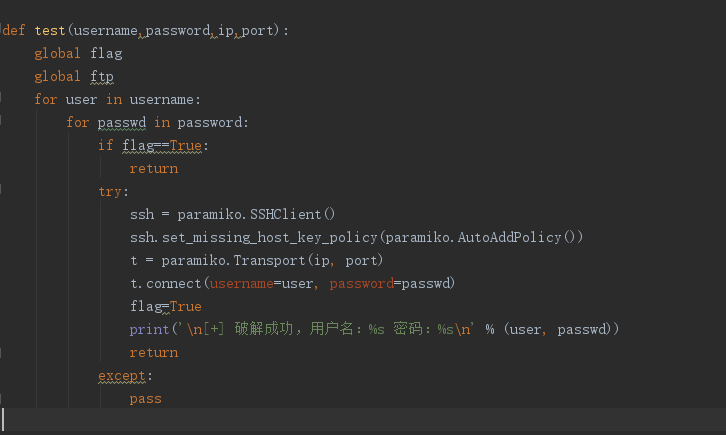
4.4.2 暴力破解

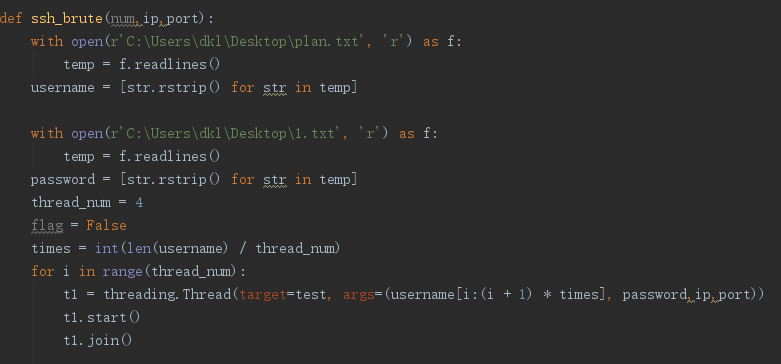
（1）ftp暴力破解：ftp暴力破解主要由两个函数实现test(username,password,ip,port)参数意义依次为：用户名集合，密码集合，目标IP，目标端口。该函数核心为两个for循环，遍历用户集与密码集的所有组合，调用[FTP.connect（ip](ftp://FTP.connect（ip)，port）函数进行尝试，通过对该函数调用结果的判断即可得出ftp口令与用户名是否合法，倘若函数调用正常，这说明用户名与密码正确，如果抛出异常，则说明不正确。Test函数还会记录尝试次数，记录的变量为count，后期将会通过这个次数判断是否存在ftp爆破漏洞，次数大于100的通常视为可爆破的。由于测试过程用到了多线程的方法，因此每次使用count时需要加锁。另一个函数ftp\_brute(thread\_num)，参数为线程个数，该函数通过线程个数与用户名个数算出每个线程测试的用户名个数，用用户名个数除以线程个数即可，算出每个线程测试的用户名数量后，将整个用户名集合分配好送到每个线程中，其中flag变量作为各线程的退出标记，当为true时退吹，为false则继续执行，当找到正确的用户名和密码后就会把flag变量设为true，关键代码如下：





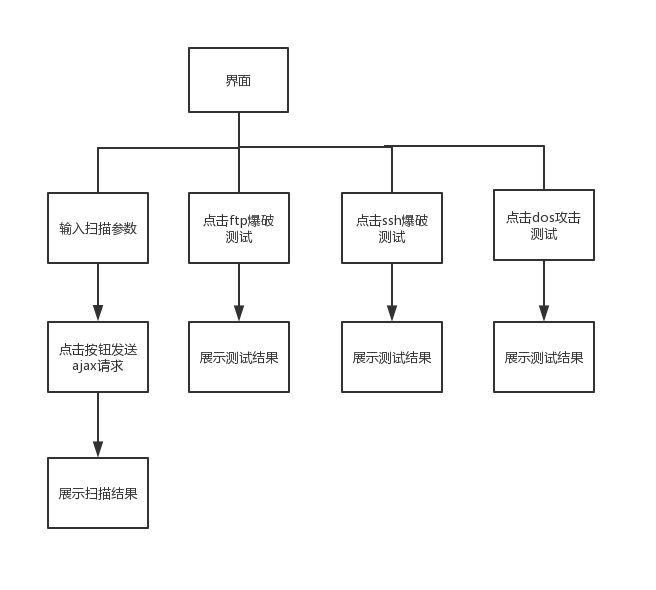
（2）ssh爆破模块，该模块主要有两个函数组成，与ftp爆破模块类似，只是所使用的的模块为paramiko模块，代码也大体同上，故而不再赘述，关键代码如下：





4.5 前端界面

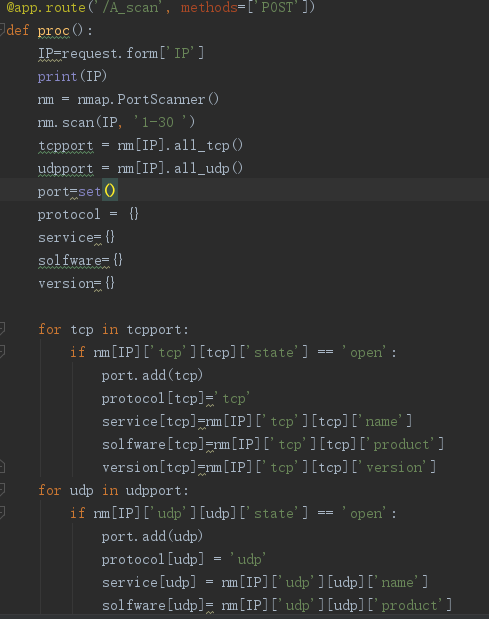
前端主要用到html/css/js以及ajax技术，核心有几个部分。首先，扫描部分：该部分有一个按钮和一个输入框，输入框接收IP,端口以及线程数量等必要的信息，并进行合法性检查，不合法的输入，软件将会给出提示帮助更正。按钮的onclick属性为一个ajax请求，该请求将输入框中的信息提交到服务端进行处理，并且等待处理后返回的数据。其次，扫描展示部分，这部分由一个组成，该表记录了扫描得出的信息，端口号、协议、服务、软件以及版本信息。再次。评估部分，该部分由一个输入框与一个按钮构成，输入框接需要接收线程数量参数，并进行合法性检查，不合法的将给出提示信息，进行爆破测试与dos攻击测试时，这个参数指明线程数量；按钮的onclick属性为一个ajax请求，该请求将输入框中的信息提交到服务端进行处理，并且等待处理后返回的数据。类似的，评估结果将会展示到评估部分后边，界面将会用js完成一些优化，使界面更优美，界面的运行流程如下：

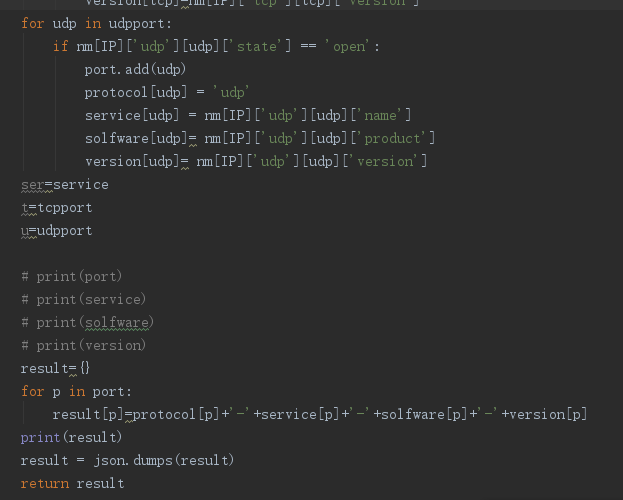


4.6 统筹模块

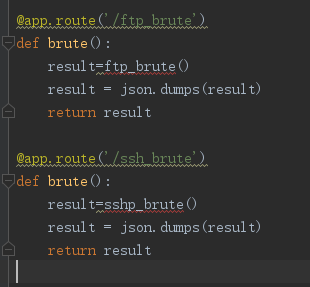
统筹模块衔接前端界面与后端功能模块，通过flask技术实现，每一个url请求用一个函数处理，主要有以下几个处理函数：

（1）处理扫描请求：扫描在前端通过ajax封装成一个post请求，处理函数首先从request.form字典读出输入参数，将IP、端口等信息分割好，调用相应的功能函数并保存好返回数据，序列化成json数据并返回前端，关键代码如下：

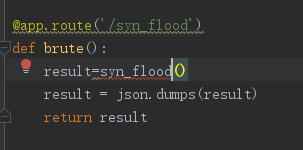




（2）处理ftp与ssh爆破，ftp与ssh爆破功能在ftp\_brute与ssh\_brute函数中大体已经完善，所以处理爆破测试只需调用并序列化返回数据即可，如下：



1. 处理dos攻击测试，类似地，调用syn\_flood函数即可：



4.7 测试环境

# 5 系统测试

5.1 扫描功能

为了测试扫描功能的完整性，做以下处理

|  |  |
| --- | --- |
| 测试用例编号 | scan\_test1 |
| 测试项目 | 网络扫描软件的扫描 |
| 输入 | 合法的IP、端口与线程数 |
| 操作 | 点击’扫描’按钮 |
| 预期结果 | 扫描信息表中各项将被填好 |

测试非法输入时的情景：

|  |  |
| --- | --- |
| 测试用例编号 | scan\_test2 |
| 测试项目 | 网络扫描软件的扫描 |
| 输入 | 非法的数据与格式 |
| 操作 | 点击’扫描’按钮 |
| 预期结果 | 弹出错误提示信息 |

5.2 ftp爆破测试

测试ftp爆破功能：

|  |  |
| --- | --- |
| 测试用例编号 | ftp\_force\_test1 |
| 测试项目 | 网络扫描软件的ftp爆破功能 |
| 输入 | IP及端口 |
| 操作 | 点击’ftp\_force’按钮 |
| 预期结果 | 显示爆破解雇及一些说明 |

测试异常情况下的ftp爆破功能：

|  |  |
| --- | --- |
| 测试用例编号 | ftp\_force\_test2 |
| 测试项目 | 网络扫描软件的ftp爆破功能 |
| 输入 | 非法的输入 |
| 操作 | 点击’ftp\_force’按钮 |
| 预期结果 | 显示错误提示 |

|  |  |
| --- | --- |
| 测试用例编号 | ftp\_force\_test3 |
| 测试项目 | 网络扫描软件的ftp爆破功能 |
| 输入 | IP及端口 |
| 操作 | 修改密码为强密码，点击’ftp\_force’按钮 |
| 预期结果 | 显示超时错误信息 |

5.3 ssh爆破测试

测试ssh爆破功能：

|  |  |
| --- | --- |
| 测试用例编号 | ssh\_force\_test1 |
| 测试项目 | 网络扫描软件的ssh爆破功能 |
| 输入 | IP及端口 |
| 操作 | 点击’ssh\_force’按钮 |
| 预期结果 | 显示爆破结果及一些说明 |

测试异常情况下的ftp爆破功能：

|  |  |
| --- | --- |
| 测试用例编号 | ssh\_force\_test2 |
| 测试项目 | 网络扫描软件的ssh爆破功能 |
| 输入 | 非法的输入 |
| 操作 | 点击’ssh\_force’按钮 |
| 预期结果 | 显示错误提醒 |

|  |  |
| --- | --- |
| 测试用例编号 | ssh\_force\_test3 |
| 测试项目 | 网络扫描软件的ssh爆破功能 |
| 输入 | IP及端口 |
| 操作 | 修改密码为强密码，点击’ssh\_force’按钮 |
| 预期结果 | 显示超时错误信息 |

5.4 dos攻击测试

测试dos攻击：

|  |  |
| --- | --- |
| 测试用例编号 | dos\_test1 |
| 测试项目 | 网络扫描软件的dos攻击测试功能 |
| 输入 | IP及端口 |
| 操作 | 点击’dos攻击’按钮 |
| 预期结果 | 打开网页变卡 |

测试非法输入时：

|  |  |
| --- | --- |
| 测试用例编号 | dos\_test2 |
| 测试项目 | 网络扫描软件的dos攻击测试功能 |
| 输入 | 非法的输入 |
| 操作 | 点击’dos攻击’按钮 |
| 预期结果 | 显示错误提示信息 |

5.4 综述

经过以上详尽的测试，软件的功能与性能要求均能符合预期；对于一些不符合预期的情况，已改进使其能正常工作。

# 6 总结

软件的开发过程中，很大一方面时间都花在了解决问题或者调试bug中，能占到一半时间左右，因而有了这个章节，梳理开发过程的困难与解决，总结经验，以求提高。另一方面对软件进行一个客观的评价，总结软件的优点以及缺点。

6.1 感想与收获

三个月前，我从对网络扫描技术只有懵懂认知到如今能独立开发一个完整的网络扫描软件，经历了许多的困难，也付出了很多，能力也得到了很大的提升。

首先，对搜索引擎的使用得到了一次升华。搜索引擎的使用看似很简单，只是输入一些关键词然后点击搜索就完了，其实里面大有学问。下面是一些总结出来的使用搜索引擎的技巧：当面对一个软件bug时，首先可以使用搜索引擎搜索报错的信息，通常我们遇到的错误，必定很多人也遇到过，搜一下报错信息通常都能找到解决问题的提示；也可以搜索一下前人的例子，看一下前任是怎么完成我这个任务的，以求触类旁通；通过前两步搜索出来的信息中的关键字，继续深入搜索；尝试英文搜索，英文是世界通用的而语言，使用英文搜索能看到更广的信息。

其次，对调试错误有了更深层次的认识。调试bug是软件开发一个重要的必经过程，虽然我们都不想经历，但通常它都汇占据总开发接近一半的时间。整个毕设坐下来，积累了许多实用的调bug的经验：面对一个Bug，首要也是最重要的是心态不能崩，要有信心和耐心；根据经验，通常很多bug都是由于程序员的疏忽所致，所以可以先去检查一下有没有简单的书写错误，大小写错误以及对齐错误等；可以根据从前出错的经验，找找出错频率较高的环节，比如内存泄露等等，仔细检查检查；可以理一下逻辑，看看是不是自己想法有问题；采用排除法，不断删减一些东西，直到定位到问题处；重新去做，有一些问题是由于理解上出现了偏差，对一个知识理解错误，通常这种错误非常难

发现，但是重新一步步去做，偶有奇效；有时候调一个bug一直没有进展，可以先放一放，去干其他的，很多时候，吃顿饭，睡一觉，洗个澡什么的，而后再回来看，会豁然开朗，从前只是有这种经历，后面了解到，这种现象其实有科学依据，因为人在长时间思考一个问题时，当天脱离了思考，他的潜意识也仍在继续思考这个问题；有时候一筹莫展之时，就需要大胆猜测问题所在，动手去逐步排查；最后还有一个办法，当实在解决不下去时，可以换一种实现，放弃这个有问题的代码，重新考虑其他办法去完成任务，或者到网上发帖求助。

同时，我对学习也有了新的认识。学习其实是一个积累与思考的过程，学习一个东西，需要积累这个东西的一些基本知识，基本处理方法与技巧，做这个东西的经验，同时还需要有思考的意识，灵活应对，以上是抽象的认识，通常抽象程度越高，或者说普适度越高，对于具体问题的解决作用就越小，但是还是得有，不然很容易就陷入迷茫，无所适从。以下是一些具体的学习的技巧或经验：从粗到细，首先掌握大概的轮廓，再通过实践或解决问题去掌握一些边边角角，比如学习新语言，就可以先大概掌握其核心语法，然后在通过项目去深化；边学边用，从前我做一个东西，总会把涉及到的知识都学了然后再来做，这样效率很低，而且没有反馈，很难坚持，采用边学边做，学以致用，这里的致使够的意思，就是说需要啥就学啥,够用就过；多看不同的版本，通常对于同一块内容，会有很多不同的表述，横向的多看看，通常很能帮助理解；遵循这个东西的特点，按照学习这个东西的规律去学习，比如编程等实践性很强的，可以多去实践，以项目来带动学习，比如学数学的时候，就需要很严谨，学英语就不能那么严谨，不能一个单词就死认那一个意思；还有就是学习挺看状态的，有时候状态不好就需要适时休息，不能和自己的硬刚，多运动可以让头脑清醒，有活力。

最后，本次毕设也让我掌握到了许多具体的技术。首先是课题相关的东西，比较深入地了解到了端口扫描与服务发现的原理与实现，对数据包与一些协议有了更深层次的理解，比如TCP三次握手、FTP协议以及HTTP协议等。毕业色阶的外文翻译环节，需要独立去寻找外文文献，通过这个环节，我的英文水准有了较大提升，能看懂专业外文文献，并且，学会了如何一些免费找找各种文献的办法，当然这得益于哈萨克斯坦的一个女研究生的杰作sci-hub。在毕设开发过程中，与同学们合作无间，沟通也略有提升，变得更开朗了。同时，由于不断的受挫，不断的想办法解决问题，我变得越来顽强，面困难也更有勇气和信心！

6.2 软件的评价与展望

本软件名为网络扫描软软件，实则已不限于网络扫描，还有一些安全的评估功能。本软件实现了基本的端口扫描，扫描处开放了哪些端口，以什么形式开放（TCP/UDP）；基本的服务发现功能，探测出各端口上运行的服务，运行服务的软件，以及软件的版本等信息，根据这些信息，可以在网上搜索到对应版本的服务或软件的漏洞。可想而知，这些信息对于对于网络的安全有多重要，对于管理员来说有多重要；软件为了优化运行的速度，运该到了多线程的技术；对于网络扫描方面，算是一个合格的网络扫描软件。除网络扫描软件的基本功能外，本软件还增加了安全评估功能，该模块对系统ftp服务以及ssh服务进行爆破测试，爆破测试原理简单，但危害巨大，随着计算机计算能力的提升，这种漏洞的危害正不断扩大；另一方面，评估模块还会能进行dos攻击测试，dos攻击由来已久，从前主要是损耗带宽，如今已经发展为损耗系统资源，本软件针对的正是系统资源的攻击，以评测系统的脆弱性。总的来说，本软件运行稳定，界面简约美观，运行速度较快，是一款合格的网络扫描软件。

然技术与知识所限，软件的不足也很明显。网络扫描是一把双刃剑，用得好，就是提升系统安全的利器，用得不好，就是潘多拉的魔盒，各种防火墙通常都会对网络扫描有一定的防范。要想对某各主机进行网络扫描，首当其冲就是得想办法绕过防火墙，而防火墙防护规则并不一致，因此，并没有通用的网络扫描软件，能够扫描所有网络上主机，本软件面对一些防火墙时也常常束手无策。同时，由于本软件主要侧重于扫描方面，漏洞扫描方面并不出色，只做了两种漏洞的检测，并且都是比较基础的漏洞，而且对于一些防火墙基本束手无策。

功与防总在不断较量中发展，网络扫描技术也在不断的发展。下一代计算机技术（量子计算）能在数小时内暴力破解强密码，传统的计算机需要数百万年；使用僵尸网络的ddos攻击使危害大幅升级；由于物联网技术的发展，越来越多物联网设备面世，智能家居，无人驾驶汽车等等。物联网的安全也获得了空前的关注，物联网安全将网络安全升华到了新的境界，从前的网络攻击，并不会对人身安全有直接影响，而如今，试想你家的微波炉被黑客控制了，汽车被黑客控制，生命安全备受威胁。与此同时，安全技术也在不断发展，列入，基于机器学习的流量识别，能更智能的识别攻击流量；云安全技术等等各种新的网络安全技术接踵而来。

网络安全，除了技术的方面，人的影响也至关重要。当今世界众多的网络攻击，很多一部分是并不是因为技术原因，而是人的原因。如前面提到的，京东2017年大量用户信息泄露，就是因为除了’内鬼’；社会工程等技术也是利用了人性的弱点，因此，在重视纯技术的同时，也应该关注人的影响。

# 谢 辞

本次毕业设计论文以及软件的完成都得到了韦必忠教授的耐心教诲，韦老师教学深刻而不失趣味，善于举生活中鲜活的例子来说明深刻的理论，把毕设的要求、重点与难点说得很清楚，同时在毕设过程中遇到的问题也对我给与了一定的帮助，倾注了大量的心血。韦老师渊博的专业知识、严谨的治学态度，精益求精的工作作风，诲人不倦的高尚师德，严于律己、宽以待人的崇高风范，朴实无法、平易近人的人格魅力也对本人影响深远，使我树立了远大的目标，掌握了扎实的理论基础，学到了许多实用的研究方法，生活作风方面也有很大改善，在韦老师的身体力行影响下，本人也开始重视运动，偶尔跑跑。在此，谨向导师表示崇高的敬意和衷心的感谢！同时，也感谢同组的小伙伴们，大家团结合作，互相交流了许多学习的心得以及一些毕设周边的小技巧，比如查重网址等，在此，也向他们表示感谢。

另外，特别感谢[哈萨克斯坦](https://zh.wikipedia.org/wiki/%E5%93%88%E8%90%A8%E5%85%8B%E6%96%AF%E5%9D%A6)研究生[亚历珊卓·艾尔巴金](https://zh.wikipedia.org/wiki/%E4%BA%9E%E6%AD%B7%E7%8F%8A%E5%8D%93%C2%B7%E8%89%BE%E7%88%BE%E5%B7%B4%E9%87%91)与其大作，Sci-Hub。亚历珊卓同学的Sci-Hub，打破了学术界的文献交流的壁垒，对全体科研人员作出了杰出的贡献，也为全人类共享知识作出了非凡贡献。同时，亚历珊卓同学不畏强权敢于斗阵的革命精神也令我深深钦佩，感谢Sci-Hub让经济局限的我及类似我的群体也能共享世界的研究精华。实际上，让科学变得更为开放，是无数有识之士共同的愿景，而免费获取科研论文就是其中的重要一环（还包括可获得更多的研究数据等），由于Sci-Hub，欧盟开始在着手发展更好的Sci-Hub，致力于到2020年，欧盟所有的科研论文均能免费获得，在此，也对[亚历珊卓·艾尔巴金](https://zh.wikipedia.org/wiki/%E4%BA%9E%E6%AD%B7%E7%8F%8A%E5%8D%93%C2%B7%E8%89%BE%E7%88%BE%E5%B7%B4%E9%87%91)对全世界科学的开放的贡献表示由衷感谢！

此外，特别感谢[理查德·斯托曼](https://zh.wikipedia.org/wiki/%E7%90%86%E6%9F%A5%E5%BE%B7%C2%B7%E6%96%AF%E6%89%98%E6%9B%BC)。理查德是自由软件运动的发起人与精神领袖，自由软件运动IT界影响深远，出现了许多优秀的开源软件，如PHP、MYSQL等，为我的毕设工作提供了有力支持，同时，若没有开源运动，恐怕也不会出现诸如scapy、nmap等一系列优秀的第三方开源库。因此，在此谨向[理查德·斯托曼](https://zh.wikipedia.org/wiki/%E7%90%86%E6%9F%A5%E5%BE%B7%C2%B7%E6%96%AF%E6%89%98%E6%9B%BC)表示崇高的敬意和衷心的感谢，也祝愿开源社区涌现越来越多的优秀软件！

最后，感谢学校对我的栽培，让我掌握了专业计算机知识，为我毕设的完成奠定了基础；感谢参考文献的编者们，他们对我毕设的完成帮助良多，如李瑞明的《网络扫描技术揭秘》直接提供了大量的技术参考；总之，感谢全体对我毕设工作有过帮助的人！