PaperTime检测报告简明打印版

相似度：13.59%
编　号：ZEIVKQEUBRJBWIJC
标　题：网络扫描软件的设计
作　者：暂无
长　度：27489字符
时　间：2019-05-26 21:59:53
比对库：本地库（学术期刊、学位论文、会议论文）；PaperTime云论文库；互联网

本地库相似资源（学术期刊、学位论文、会议论文）
1. 相似度：0.27%　篇名：《基于端口扫描的安全漏洞检测系统的设计与实现》
来源：《山东大学硕士学位论文》　年份：2005　作者：刘成志
2. 相似度：0.24%　篇名：《基于FTP协议的文件传输组件设计与实现》
来源：《沈阳师范大学学报：自然科学版》　年份：2012　作者：王占军
3. 相似度：0.23%　篇名：《智能家居更新事务管理系统的研究与开发》
来源：《东南大学硕士学位论文》　年份：2017　作者：张虹
4. 相似度：0.22%　篇名：《Java网络通信对ICQ的实现》
来源：《计算机光盘软件与应用》　年份：2013　作者：杨敏
5. 相似度：0.21%　篇名：《浅析光纤网络的路由通信协议》
来源：《中国科技投资》　年份：2013　作者：关滨
6. 相似度：0.18%　篇名：《TCP/IP下DDOS检测与防御技术的研究》
来源：《河北工程大学硕士学位论文》　年份：2011　作者：张德杨
7. 相似度：0.16%　篇名：《基于MongoDB的保险销售管理系统的设计与实现》
来源：《湖南大学硕士学位论文》　年份：2016　作者：邹明明
8. 相似度：0.13%　篇名：《面向安卓的人机交互模块生成器的研究与实现》
来源：《北京邮电大学硕士学位论文》　年份：2016　作者：刘晓佳
9. 相似度：0.13%　篇名：《基于SSL协议的FTP服务器设计与实现》
来源：《中国地质大学(北京)硕士学位论文》　年份：2016　作者：韦超
10. 相似度：0.11%　篇名：《浅谈ORACLE数据库管理》
来源：《信息系统工程》　年份：2013　作者：张墨晖
11. 相似度：0.11%　篇名：《基于本体和属性攻击图的渗透测试模型研究与系统实现》
来源：《重庆大学硕士学位论文》　年份：2013　作者：胡兵
12. 相似度：0.10%　篇名：《Windows系统网络安全扫描工具的设计与实现》
来源：《北京工业大学硕士学位论文》　年份：2013　作者：朱蓉
13. 相似度：0.09%　篇名：《基于语义的P2P搜索研究与仿真实现》
来源：《电子科技大学硕士学位论文》　年份：2011　作者：孟振中
14. 相似度：0.09%　篇名：《基于网络加密卡的传输层基本协议研究》
来源：《黑龙江大学硕士学位论文》　年份：2012　作者：刘冠君
15. 相似度：0.09%　篇名：《综合扫描系统的设计与实现》
来源：《电子科技大学硕士学位论文》　年份：2017　作者：陈昊
16. 相似度：0.09%　篇名：《正则表达式及其应用》
来源：《电脑编程技巧与维护》　年份：2012　作者：马永萍
17. 相似度：0.08%　篇名：《浅谈小学班主任德育工作》
来源：《散文百家：下旬刊》　年份：2017　作者：宋彦红
18. 相似度：0.08%　篇名：《基于REST的虚拟空间天气观测台数据接口研究》
来源：《中国地质大学（北京）硕士学位论文》　年份：2013　作者：巨枫
19. 相似度：0.08%　篇名：《Java网络编程语言的应用流程探讨》
来源：《计算机光盘软件与应用》　年份：2014　作者：周涛赋
20. 相似度：0.08%　篇名：《特定WEB漏洞分析系统研究与实现》
来源：《南京邮电大学硕士学位论文》　年份：2017　作者：别宜东
21. 相似度：0.08%　篇名：《面向抗攻击测试的攻击语言设计与实现》

来源：《解放军信息工程大学硕士学位论文》 年份：2008 作者：辛思远
22. 相似度：0.07% 篇名：《基于嵌入式浏览器的JS引擎移植的研究与应用开发》
来源：《天津大学硕士学位论文》 年份：2009 作者：张宏伟
23. 相似度：0.07% 篇名：《基于$3C2440平台搭建linux环境》
来源：《通信技术》 年份：2013 作者：冯开林
24. 相似度：0.07% 篇名：《Linux服务器配置》
来源：《计算机光盘软件与应用》 年份：2014 作者：李治西
25. 相似度：0.06% 篇名：《Linux环境下FTP系统的设计与实现》
来源：《吉林大学硕士学位论文》 年份：2012 作者：李杰
26. 相似度：0.06% 篇名：《Flask框架下成品油销售系统设计与实现》
来源：《西安电子科技大学硕士学位论文》 年份：2015 作者：王译庆
27. 相似度：0.06% 篇名：《基于云存储的Web OS浏览器的研究和实现》
来源：《华南理工大学硕士学位论文》 年份：2012 作者：熊磊
28. 相似度：0.05% 篇名：《基于高效的SSH协议的运维审计系统研究与实现》
来源：《湖南大学硕士学位论文》 年份：2011 作者：张红
29. 相似度：0.05% 篇名：《动态语言Python探讨与比较》
来源：《企业科技与发展：上半月》 年份：2012 作者：张茗芳
30. 相似度：0.05% 篇名：《TCP / IP原理和Syn攻击防范》
来源：《计算机光盘软件与应用》 年份：2011 作者：朱达
31. 相似度：0.04% 篇名：《移动Agent在电子商务平台中的应用》
来源：《湖北工业大学硕士学位论文》 年份：2009 作者：刘恒峰
32. 相似度：0.04% 篇名：《便携式水质现场测试仪的驱动开发》
来源：《郑州大学硕士学位论文》 年份：2016 作者：杨东升
33. 相似度：0.04% 篇名：《基于Linux平台FTP搜索引擎的研究》
来源：《湖北工业大学硕士学位论文》 年份：2009 作者：黎冬
34. 相似度：0.04% 篇名：《大数据时代的信息安全风险与防护》
来源：《计算机光盘软件与应用》 年份：2014 作者：于慧勇
35. 相似度：0.04% 篇名：《基于Web的高职院校评估工作管理信息系统的设计与实现》
来源：《西北农林科技大学硕士学位论文》 年份：2013 作者：段存乾
36. 相似度：0.04% 篇名：《基于FC协议的FDMI模块的设计与实现》
来源：《华中科技大学硕士学位论文》 年份：2014 作者：李翀
37. 相似度：0.04% 篇名：《基于SNMP网络安全管理研究》
来源：《河南大学硕士学位论文》 年份：2008 作者：黄晓巧
38. 相似度：0.04% 篇名：《电信宽带城域网网络安全体系的研究》
来源：《江南大学硕士学位论文》 年份：2007 作者：孙玫
39. 相似度：0.04% 篇名：《新型网络攻击实验平台关键技术的研究与实现》
来源：《华南师范大学硕士学位论文》 年份：2007 作者：龙灿
40. 相似度：0.04% 篇名：《Ajax实现数据交互技术》
来源：《网友世界》 年份：2015 作者：何祥宇
41. 相似度：0.04% 篇名：《IP网脆弱性分析及安全控制策略的研究》
来源：《中国石油大学硕士学位论文》 年份：2010 作者：穆韶山
42. 相似度：0.04% 篇名：《一种Java多线程可达性测试框架系统的研究和实现》
来源：《暨南大学硕士学位论文》 年份：2003 作者：李双权
43. 相似度：0.04% 篇名：《基于Lucene的中英文文档全文搜索引擎》
来源：《电子科技大学硕士学位论文》 年份：2008 作者：张瑞
44. 相似度：0.03% 篇名：《宽带收发单元的控制系统软件》
来源：《电子科技大学硕士学位论文》 年份：2015 作者：徐驰

PaperTime云论文库(知网，万方，维普，百度文库等镜像）

1. 相似度：0.18% 标题：《毕业论文谢辞 - 道客巴巴》
来源：http://www.doc88.com/p-69423272885.html

互联网相似资源(博客，百科，论坛，新闻等）

1. 相似度：0.55% 标题：《毕设论文致谢.doc -max上传文档投稿赚钱-文档C2C交易模式-100%...》

来源：http://max.book118.com/html/2017/0611/113449417.shtm
2. 相似度：0.54% 标题：《毕业论文致谢信致谢词范文精选12篇模板_绿色文库网》
来源：http://wenku.cyjzzd.com/a/1300001727
3. 相似度：0.43% 标题：《LAMP搭建系列二、Apache安装 (apt) - 简书》
来源：https://www.jianshu.com/p/c5db66973c6d
4. 相似度：0.36% 标题：《欧盟欲推“正版”Sci-Hub,《Science》网站评论区再炸……_新浪博客》
来源：http://blog.sina.com.cn/s/blog_1509e343b0102wghf.html
5. 相似度：0.36% 标题：《FreeNAS的TFTP使用篇- tomora的专栏- CSDN博客》
来源：https://blog.csdn.net/tomora/article/details/11703023
6. 相似度：0.33% 标题：《Python实现SSH远程登陆,并执行命令! - pfm685757的专栏 - CSDN博客》
来源：https://blog.csdn.net/pfm685757/article/details/60880039
7. 相似度：0.32% 标题：《论文答谢语》
来源：https://www.lz13.cn/lizhiyanjiang/57942.html
8. 相似度：0.32% 标题：《CNCERT发布《2018年我国互联网网络安全态势报告》_手机搜狐网》
来源：http://m.sohu.com/a/308806980_120027127/
9. 相似度：0.30% 标题：《SSH 协议原理、组成、认证方式和过程- 技术学习- 简书》
来源：https://www.jianshu.com/p/8e5b7aea52b5
10. 相似度：0.27% 标题：《ubuntu环境下使用apt-get配置apache+php+mysql - 李长鸿- 博客园》
来源：https://www.cnblogs.com/huntaiji/p/4897528.html
11. 相似度：0.27% 标题：《科学网—打破科学引文“付费墙”:开放获取新进展 - Enago英论阁的...》
来源：http://blog.sciencenet.cn/blog-681387-1049699.html
12. 相似度：0.26% 标题：《黑翼博客- 特立独行》
来源：http://www.hack1412.com/
13. 相似度：0.25% 标题：《FTP与Http的区别_百度知道》
来源：https://zhidao.baidu.com/question/7088238.html
14. 相似度：0.24% 标题：《ubuntu系统的sudo apt-get install vsftpd安装命令安装..._百度知道》
来源：https://zhidao.baidu.com/question/1926241131101544547.html
15. 相似度：0.24% 标题：《什么是网络安全,常用的安全措施有那些?求答案!急!_百度知道》
来源：https://zhidao.baidu.com/question/1302046757127505459.html
16. 相似度：0.23% 标题：《linux下开启SSH,并且允许root用户远程登录,允许无密码..._CSDN博客》
来源：https://blog.csdn.net/zilaike/article/details/78922524
17. 相似度：0.23% 标题：《做python Web开发你要理解:WSGI & uwsgi》
来源：https://www.jianshu.com/p/679dee0a4193
18. 相似度：0.22% 标题：《使用VB实现上传下载功能,要求使用SSH协议》
来源：https://bbs.csdn.net/topics/391932214
19. 相似度：0.22% 标题：《SSH 学习记录及在SSH模式下使用XShell连接服务器- 九二- 博客园》
来源：https://www.cnblogs.com/lomper/p/4600395.html
20. 相似度：0.21% 标题：《ssl与ssh - 指尖的乐律 - 博客园》
来源：https://www.cnblogs.com/zjdyl/p/4168258.html
21. 相似度：0.18% 标题：《<script src="https://code.jquery.com/jquery.js"></s..._百度知道》
</br> 来源：https://zhidao.baidu.com/question/1371193226357709339.html
</br> 22. 相似度：0.17% 标题：《HTML(Hyper Text Markup Language)超文本标记语言 - 16..._CSDN博客》
</br> 来源：https://blog.csdn.net/xiaoxiangyu5/article/details/46805713
</br> 23. 相似度：0.16% 标题：《点击提交按钮触发ajax请求时,做到处理完前一个请求后再..._CSDN博客》
</br> 来源：https://blog.csdn.net/everything1209/article/details/39250485
</br> 24. 相似度：0.15% 标题：《AJAX面试题都在这里 - 简书》
</br> 来源：https://www.jianshu.com/p/1e147aba6c31
</br> 25. 相似度：0.15% 标题：《前端js如何发起http请求后端后端- Stony_Confident的博客- CSDN博客》
</br> 来源：https://blog.csdn.net/stony_confident/article/details/79056649
</br> 26. 相似度：0.15% 标题：《Windows下安装Kali Linux (双系统) - CSDN博客》
</br> 来源：https://blog.csdn.net/qq_31386215/article/details/69664759?fps=1&locationNum=7
</br> 27. 相似度：0.15% 标题：《FTP服务器(文件访问,文件下载,文件上传) - 静陌慕春 - CSDN博客》
</br> 来源：https://blog.csdn.net/qq_39295755/article/details/81536874
</br> 28. 相似度：0.15% 标题：《关于kali开机自动启动ssh服务的方法以及配置kalissh的..._CSDN博客》
</br> 来源：https://blog.csdn.net/myfox0630/article/details/51958505
</br> 29. 相似度：0.15% 标

题：《Metasploit终端下的辅助扫描工具 (auxiliary模块讲解) ..._CSDN博客》
</br> 来源：https://blog.csdn.net/Aaron_Miller/article/details/80535992
</br> 30. 相似度：0.15% 标题：《CSS基础- 简书》
</br> 来源：https://www.jianshu.com/p/08da7ecb6ef2
</br> 31. 相似度：0.15% 标题：《关于CSS的那些事- weixin_33690963的博客- CSDN博客》
</br> 来源：https://blog.csdn.net/weixin_33690963/article/details/88747152
</br> 32. 相似度：0.15% 标题：《FTP服务使用得端口有那些_百度知道》
</br> 来源：https://zhidao.baidu.com/question/215325132.html
</br> 33. 相似度：0.15% 标题：《give的短语- 简书》
</br> 来源：https://www.jianshu.com/p/fe947711f501
</br> 34. 相似度：0.14% 标题：《AJAX http请求XMLHttpRequest - qq_35745321的博客- CSDN博客》
</br> 来源：https://blog.csdn.net/qq_35745321/article/details/52075193
</br> 35. 相似度：0.14% 标题：《Ubuntu下安装和配置Apache2 - 真理部 - CSDN博客》
</br> 来源：https://blog.csdn.net/jb19900111/article/details/17787789
</br> 36. 相似度：0.14% 标题：《【Python】学习笔记——-20、Web开发 - 你只管努力, - CSDN博客》
</br> 来源：https://blog.csdn.net/singit/article/details/60138698
</br> 37. 相似度：0.13% 标题：《Ubuntu 安装R和Rstudio Server(重要) gavin cdc的博客 CSDN博客》
</br> 来源：https://blog.csdn.net/gavin_cdc/article/details/88982293
</br> 38. 相似度：0.13% 标题：《安装kali Linux 2018.2以后的事- 苏寅的博客- CSDN博客》
</br> 来源：https://blog.csdn.net/qq_34562959/article/details/80941426
</br> 39. 相似度：0.12% 标题：《www.sec.gov》
</br> 来源：https://www.sec.gov/Archives/edgar/data/1577552/000104746918005257/a2235254z20-f.htm
</br> 40. 相似度：0.12% 标题：《用Python编写端口扫描器- wz_cow的博客- CSDN博客》
</br> 来源：https://blog.csdn.net/wz_cow/article/details/80834618
</br> 41. 相似度：0.11% 标题：《Linux基础sshd服务- Minligang - 博客园》
</br> 来源：https://www.cnblogs.com/minligang539/p/10679838.html
</br> 42. 相似度：0.11% 标题：《ssh 远程登陆指定端口 - z69183787的专栏 - CSDN博客》
</br> 来源：https://blog.csdn.net/z69183787/article/details/76153247
</br> 43. 相似度：0.11% 标题：《深入理解FTP协议 - luoxn28 - 博客园》
</br> 来源：https://www.cnblogs.com/luoxn28/p/5585458.html
</br> 44. 相似度：0.11% 标题：《互联网带来生活便利的同时,也给普通人带来了逆袭的机会》
</br> 来源：https://blog.csdn.net/zh634455283/article/details/86568097
</br> 45. 相似度：0.10% 标题：《帮忙翻译一下这个摘要,论文上用,谢谢~~~_百度知道》
</br> 来源：https://zhidao.baidu.com/question/536021368.html
</br> 46. 相似度：0.10% 标题：《HTML中javascript的<script>标签使用方法详解 - Prettiest - 博客园》
</br> 来源：https://www.cnblogs.com/Prettiest/p/7115164.html
</br> 47. 相似度：0.10% 标题：《Linux系统10个开源漏洞检测工具 大坏蛋的博客 CSDN博客》
</br> 来源：https://blog.csdn.net/weixin_41515615/article/details/84619969
</br> 48. 相似度：0.10% 标题：《mysql执行mysql root p出现Access denied for use.》
</br> 来源：https://www.jianshu.com/p/22e759996b10
</br> 49. 相似度：0.10% 标题：《求教python程序调用scapy模块的问题-CSDN论坛》
</br> 来源：https://bbs.csdn.net/topics/390780640
</br> 50. 相似度：0.10% 标题：《SSH2.0编程 ssh协议过程实现(转) - 沧海一滴 - 博客园》
</br> 来源：https://www.cnblogs.com/softidea/p/4550552.html
</br> 51. 相似度：0.10% 标题：《如何开启SSH SERVER服务_百度知道》
</br> 来源：https://zhidao.baidu.com/question/2118037596478107187.html
</br> 52. 相似度：0.09% 标题：《ubuntu 如何修改etc/apt/sources.list?_百度知道》
</br> 来源：https://zhidao.baidu.com/question/369742333093975684.html
</br> 53. 相似度：0.09% 标题：《TCP握手与socket通信细节》
</br> 来源：https://www.jianshu.com/p/3f42172f582b
</br> 54. 相似度：0.08% 标题：《00后男孩约网友遭仙人跳如何看待未成年教育问题|男孩|网友-滚动...》
</br> 来源：http://www.guangyuanol.cn/news/newspaper/2018/0825/890640.html
</br> 55. 相似度：0.08% 标题：《中级软件设计师备考 Dark's World CSDN博客》
</br> 来源：https://blog.csdn.net/ivandark/article/details/8493348
</br> 56. 相似度：0.08% 标题：《python模块学习---nmap模块_慕课手记》
</br> 来源：https://www.imooc.com/article/45378
</br> 57. 相似度：0.08% 标题：《怎样启动windows 防火墙_百度知道》
</br> 来源：https://zhidao.baidu.com/question/5392867.html
</br> 58. 相似度：0.07% 标题：《Kali Linux允许root ssh登录》
</br> 来源：https://www.jianshu.com/p/df6101fbafeb
</br> 59. 相似度：0.07% 标题：《WSGI的理解 不走弯路,就是捷径! CSDN博客》
</br> 来源：

https://blog.csdn.net/hzrandd/article/details/10099871
</br> 60. 相似度：0.07% 标题：《onclick事件的传值 然后去执行ajax请求 - yikeshuo的博..._CSDN博客》
</br> 来源：https://blog.csdn.net/pgke915/article/details/50947187
</br> 61. 相似度：0.07% 标题：《VMware Workstation:安装windows xp系统 nicergj的博客 CSDN博客》
</br> 来源：https://blog.csdn.net/nicergj/article/details/83651603
</br> 62. 相似度：0.07% 标题：《ssh详细的介绍SSH的英文全称是Secure Shell Hibernate-CSDN下载》
</br> 来源：https://download.csdn.net/download/ale26/3082854
</br> 63. 相似度：0.07% 标题：《僵尸网络入侵智能物联网设备的趋势分析 - 墨者安全 - 博客园》
</br> 来源：https://www.cnblogs.com/mozheanquan/p/10119730.html
</br> 64. 相似度：0.07% 标题：《Linux系统和Windows系统有什么区别,为什么在Windows系..._百度知道》
</br> 来源：https://zhidao.baidu.com/question/1047913954762598819.html
</br> 65. 相似度：0.07% 标题：《两会关注信息安全,面对隐患企业可以这样做》
</br> 来源：https://baijiahao.baidu.com/s?id=1594336869786592226&wfr=spider&for=pc
</br> 66. 相似度：0.06% 标题：《php利用curl发起get请求时url的参数问题 - SegmentFault 思否》
</br> 来源：https://segmentfault.com/q/1010000006901951
</br> 67. 相似度：0.06% 标题：《python是什么语言_百度知道》
</br> 来源：https://zhidao.baidu.com/question/14270501.html
</br> 68. 相似度：0.06% 标题：《假设你在编写一个使用多线程技术的程序,当程序中止运行时,需要》
</br> 来源：https://www.nowcoder.com/questionTerminal/2ca35542a3294127bfbbe6c974b86eb7?orderByHotValu
</br> 69. 相似度：0.06% 标题：《对学习文言文的看法_百度知道》
</br> 来源：https://zhidao.baidu.com/question/27670994.html
</br> 70. 相似度：0.05% 标题：《网络协议8 - TCP协议(上):性恶就要套路深- 北国丶风光- 博客园》
</br> 来源：https://www.cnblogs.com/BeiGuo-FengGuang/p/10029735.html
</br> 71. 相似度：0.05% 标题：《Nmap 讲解从简到难---04:进行防火墙绕过,Web服务审计,W..._CSDN博客》
</br> 来源：https://blog.csdn.net/m0_37268841/article/details/80405161
</br> 72. 相似度：0.05% 标题：《26岁的狮子瑞星过得可好,还有机会吗?_搜狐科技_搜狐网》
</br> 来源：http://it.sohu.com/20180108/n527548314.shtml
</br> 73. 相似度：0.05% 标题：《Python学习笔记- 爱做梦的鱼- 博客园》
</br> 来源：https://www.cnblogs.com/dreamer-fish/p/3821762.html
</br> 74. 相似度：0.05% 标题：《TCP:三次握手,URG、ACK、PSH、RST、SYN、FIN 含义- 翼紫珊- ...》
</br> 来源：https://blog.csdn.net/wudiyi815/article/details/8505726
</br> 75. 相似度：0.05% 标题：《linux下端口扫描的实现(TCP connect、TCP SYN、TCP FIN..._CSDN博客》
</br> 来源：https://blog.csdn.net/xy913741894/article/details/77254805
</br> 76. 相似度：0.05% 标题：《软件测试面试题(一) - LY2018 - 博客园》
</br> 来源：https://www.cnblogs.com/ly2018/p/8572829.html
</br> 77. 相似度：0.05% 标题：《在linux下登录ssh怎么指定端口_百度知道》
</br> 来源：https://zhidao.baidu.com/question/1950582611941019548.html
</br> 78. 相似度：0.05% 标题：《Nmap扫描软件分析 - Birldlee的博客 - CSDN博客》
</br> 来源：https://blog.csdn.net/Birldlee/article/details/78907934
</br> 79. 相似度：0.05% 标题：《【起点抢任务软件和天眼网络探手哪个好用】起点抢任务软件和天眼...》
</br> 来源：http://xiazai.zol.com.cn/pk/420945_371309.shtml
</br> 80. 相似度：0.05% 标题：《html页面post数据到服务端(socket接收),socket获取之后..._CSDN论坛》
</br> 来源：https://bbs.csdn.net/topics/390820789
</br> 81. 相似度：0.05% 标题：《FTP的20、21端口,工作模式 Rain CSDN博客》
</br> 来源：https://blog.csdn.net/lanmolei814/article/details/49912629
</br> 82. 相似度：0.05% 标题：《Python paramiko 模块详解与SSH主要功能模拟 - u014028..._CSDN博客》
</br> 来源：https://blog.csdn.net/u014028063/article/details/81197431
</br> 83. 相似度：0.05% 标题：《“亮剑”网络顽疾》
</br> 来源：http://www.sohu.com/a/120244688_118608
</br> 84. 相似度：0.05% 标题：《Nmap扫描原理与用法(上)_91Ri.org》
</br> 来源：http://www.91ri.org/8654.html
</br> 85. 相似度：0.04% 标题：《网络安全的重要性_百度知道》
</br> 来源：https://zhidao.baidu.com/question/1541293155588948507.html
</br> 86. 相似度：0.04% 标题：《常见的端口扫描类型及原理》
</br> 来源：http://www.360doc.com/content/12/0302/13/3725126_191092221.shtml
</br> 87. 相似度：0.04% 标题：《【Python3网络爬虫开发实战】3.1.1-发送请求- 知乎》
</br> 来源：https://zhuanlan.zhihu.com/p/33876599
</br> 88. 相似度：0.04% 标题：《输入两个字符串

str1和str2,(str1>str2),判断str1里面是..._CSDN论坛》
</br> 来源：
https://bbs.csdn.net/topics/390234850
</br> 89. 相似度：0.04% 标题：《简述Get提交方式和Post提交方式有哪些不同 - m0_376683..._CSDN博客》
</br> 来源：
https://blog.csdn.net/m0_37668335/article/details/80556885
</br> 90. 相似度：0.04% 标题：《由大型物联网僵尸网络驱动的DDoS攻击_搜狐科技_搜狐网》
</br> 来源：
http://www.sohu.com/a/116688470_354899
</br> 91. 相似度：0.04% 标题：《学习总结HTML CSS JAVASCRIPT,对三剑客的一些理解 - 勿在浮沙筑...》
</br> 来源：
https://blog.csdn.net/u013565163/article/details/51062051
</br> 92. 相似度：0.04% 标题：《FTP主动模式与被动模式 - CSDN博客》
</br> 来源：
https://blog.csdn.net/windlyb/article/details/7786446
</br> 93. 相似度：0.04% 标题：《Ubuntu 中 Apache2 安装、配置、卸载 - 马帅的博客 - CSDN博客》
</br> 来源：
https://blog.csdn.net/mashuai720/article/details/83030647
</br> 94. 相似度：0.04% 标题：《kali linux 下python3.6.2+pip3配置安装- zhangxiaoshuoyu的博客- ...》
</br> 来源：
https://blog.csdn.net/zhangxiaoshuoyu/article/details/76222950
</br> 95. 相似度：0.04% 标题：《什么是SSH协议,ssh协议加解密方式》
</br> 来源：
https://www.jianshu.com/p/5a5f34489690
</br> 96. 相似度：0.04% 标题：《基于WEB平台的电子招投标信息管理系统设计与实现-软件工程专业...》
</br> 来源：
https://max.book118.com/html/2019/0214/8000012050002006.shtm
</br> 97. 相似度：0.04% 标题：《TCP三次握手详解及释放连接过程(“三次握手”和“四次挥手”)》
</br> 来源：
https://blog.csdn.net/weixin_42805929/article/details/81607399
</br> 98. 相似度：0.04% 标题：《在vSphere Client上安装虚拟机工具VMware Tools_Linux教程_Linux...》
</br> 来源：
https://www.linuxidc.com/Linux/2016-07/133245.htm
</br> 99. 相似度：0.03% 标题：《FTP协议及工作原理详解 - weixin_34413065的博客 - CSDN博客》
</br> 来源：
https://blog.csdn.net/weixin_34413065/article/details/87081448
</br>
</br> 全文简明报告
</br>
</br> 摘 要 {98% : 当今社会，网络已经渗透到生活的各个方面。 }支付宝的创立，标志着网络进一步深入人们生活当中。{ 57% : 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。{ 79% : 人们对网络安全重视达到空前高度， }网络扫描软件应运而生。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，得出端口和服务的基本信息，同时还对系统进行脆弱性检测，帮助使用者更好的管理系统，维护系统安全。 本软件采用B/S架构，用户只需在浏览器上输入域名，即可进入软件界面，进行系统脆弱性检查，同时能获得针对性的改进建议，以完善系统的安全防护。系统交互界面大方美观，对用户亲切友善，运行准确迅速。本软件前端界面采用html/css/js完成，数据通过ajax技术异步交互；后端采用scapy模块定制特定的探针协议包，将构造好的数据包由scapy模块哦发送出去，通过对数据包的分析嗅探出端口的开放信息，服务的开发信息。系统脆弱性检查由对主机进行常规漏洞的模拟测试完成，如syn泛洪，暴力破解等。 关键词：B/S；网络扫描；网络安全 Abstract In today's society, the network has penetrated into all aspects of life. The creation of Alipay marked the further development of the Internet in people's lives.{ 59% : While enjoying the convenience of the Internet, } some security issues are becoming increasingly acute. In April 2017, Youku has 10 million user account information be sold on the secret network; in March of the same year, 58 people TongCheng disclosed major personal information leaks, 700 yuan can see everyone's resume. People attach great importance to network security to an unprecedented level, and network scanning software emerges as the times require. Network scanning software is a kind of network security software. It scans local or remote computer systems to get the basic information of ports and services. At the same time, it also detects the vulnerability of the system to help users better manage the system and maintain system security. This software adopts B/S architecture. Users can enter the software interface and check the vulnerability

of the system by simply entering the domain name on the browser. At the same time, they can get targeted improvement suggestions to improve the security of the system. The interactive interface of the system is generous and beautiful. It is friendly to users and runs accurately and quickly. The front-end interface of the software is completed by html/css/js, and the data is interacted asynchronously through Ajax technology; the back-end uses scapy module to customize the specific probe protocol package, and sends the constructed data package by scapy module.{ 57% : Through the analysis of the data packet, } the open information of the port and the development information of the service are detected. System vulnerability checking is accomplished by simulating the conventional vulnerabilities of the host, such as syn flooding, violent cracking, etc.. Key words: B/S; network scanning; network secure 目 录 引言 1 1 课题背景及调研情况 2 1.1研究背景及意义 2 1.2 发展现状 2 1.4 可行性分析 3 1.5 论文的组织 3 2 开发技术 5 2.1 前端技术 5 2.1.1 HTML和CSS 5 2.1.2 JavaScript和AJAX 5 2.2 后端技术 6 2.2.1 后端框架 6 2.2.1 python编程技术 6 2.3 开源库 7 2.3.1 nmap与python-nmap 7 2.3.2 scapy 7 2.3.3 request 7 2.3.4 FTP 7 2.3.5 paramiko 7 2.4 端口扫描技术 8 2.4.1完全连接扫描 8 2.4.2 syn半连接扫描 8 2.5 服务发现技术 8 2.5.1 ftp服务发现 8 2.5.2 ssh服务发现 8 2.5.3 web服务发现 9 2.6 网络攻击技术 9 2.6.1 爆破测试 9 2.6.2 dos攻击 9 2.7 Linux技术 9 2.8 涉及到的网络协议 10 2.8.1 tcp三次握手 10 2.8.2ftp协议 10 2.8.3 ssh协议 11 2.8.4 http协议 12 2.8.5WSGI规范 12 2.9 正则表达式 13 3 需求分析 14 3.1输入输出需求 14

引言 { 63% : 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[13]。 }{ 55% : 当今全球网络安全形势日益严酷， }国家对网络安全空前重视。鉴于这样的背景，网络扫描软件就显得十分重要了。它能扫描出系统的基本安全情况，为系统使用者保障系统安全提供给了必要的参考信息。 论文设计完成一个采用B/S模式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，评估模块针对扫描结果，进行一系列模拟攻击测试，以检测出系统的脆弱性情况。本软件选取轻量级的Flask框架技术作为后端主要技术。{ 59% : 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。{ 61% : 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。{ 66% : 前后端通信采用ajax异步技术，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。为了系统的运行速度能够更快，系统采用了并发技术，具体由多线程实现。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、数据结构、设计流程、系统可用性及稳定性的测试等，选取核心的部份进行介绍。   1 课题背景及调研情况 1.1研究背景及意义 { 76% : 随着计算机与网络的不断发展， }互联网越发深入的影响人们的生活。人们在网上；浏览新闻，看视频听音乐等娱乐活动；在网上协同办公，或在腾讯文档上协同完成文档报告，{ 56% : 或在GitHub上共同完成软件； }也在网上处理各种日常事务，如使用支付宝为商品付款，在淘宝京东上购物等，可以说，网络已经彻底变为当今人人们生活必不可少的东西了。此外，物联网发展趋势如日中天，各种智能家居、智能家电等更是如雨后春笋般涌出。{ 76% : 人们在享受互联网便利的同时，}安全方面的问题日益尖锐起来。 近年来，互联网安全问题日渐尖锐，已经危害到了到政治、经济、社会甚至是人身等多个方面，全球对网络安全监管力度直线上升，不断出台各种新的政策法规，去年，{ 62% : 由中央网络安全和信息化委员会牵头，我国深化网络安全和信息化管理，各行业相关部门协作推进网络安全治理。 }然而，整个互联网的天空中还是飘着几片乌云，勒索病毒攻击事件频发，各种变种层出不穷，个人和企业饱受其害，比如前年，通过”永恒之蓝”漏洞扩散出去的wannacry敲诈程序，席卷九州，造成了不可估量的经济破坏；根据可信报告，{ 56% : 2018年全球收到的各类高级威胁报告较2017年增长了了3.6倍， }攻击呈现很强的地域特征，集中在中东和亚太等政治色彩强烈的地方，{ 64% : 受攻击的领域也多是部队国防、政治、外交及能源等， }严重危害国防安全；去年3月，美国巨无霸企业FaceBook被爆出现大量的的数据外泄，这些数据被别有用力的人运用，给无数用户造成了巨大困扰。同时，我国电商巨头京东也爆出大规模用户信息泄露，对个人的隐私造成极大损害，这也间接导致了无数的电信诈骗，骚扰电话等等。 网络深入生活，而安全问题却异常尖锐，{ 55% : 在这样的背景下，网络扫描软件应运而生， }致力于帮助企业管理员，更自动化更好的管理系统；帮助个人用户，更好的维护隐私信息的安全。网络扫描软件将本地或者远程系统的端口开放情况，服务开放情况等信息扫描出来，让使用者更加方便、全面的掌握计算机安全信息；软件同时会根据信息，对主机开展针对性的脆弱性检测，{ 57% : 让用户了解系统存在的一些漏洞等， }同时给出相应的加固建议，以协助管理人员更方便的维护系统的安全。 1.2 发展现状 目前市面上的扫描软件大致存在两种，一块是360为首的安全扫描软件，这些软件主要针对系统是否存在病毒木马进行扫描，同时检测主机的修补漏洞更新是不是最近时间的。扫描全面但耗时长久，对网络方面的扫描涉及不多，针对性不强；另一块扫描软件主要集中刚在Linux系统中，Linux系统中有无数的优秀的扫描软件，不管是像360那样全面而耗时长久的，或是仅仅针对端口或者服务进行单一扫描的，一应俱全。然而，这却有一个致命的弱点，{ 72% : Linux系统相比于Windows系列系统， }对用户极不友好，没有图形界面，普通用户断然使用不来。因而，{ 59% : Windows下网络扫描软件少， }而且太笨重；Linux中优秀软件平常使用者又无法使用。 1.3 本文主要工作 （1）阐明网络扫描软件的开发背景、意义以及网络扫描软件发展现状。 （2）说明开发中用到的编程思想以及相关技术，记录整个系统的开发过程，以及一些收获与体会。 （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。 （5）总结软件开发的心路历程以及收获。 （6）给出本软件的客观评价与技术展望。 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，然而软件本身是合法的，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 { 65% : 本文总共分为七章，各章节的大致内容如下： } 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、发展现状、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：给出网络扫描软件的需求分析。 第四章：给出软件的系统设计，介绍各模块的大致用处。 { 57% : 第五章：描述软件详细实现情况。 } 第六章：测试软件功能与效率，{ 60% : 包括扫描测试及评估测试，分析测试结果。 } 第七章：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 {90% : 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。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。新出来的HTML5可以插入图片或者视频，使网页更加丰富多彩。HTML功能强大，但使用却并不复杂，它不像其他开发语言那样有繁复的语法，它由各种元素构成，通过对元素的内容进行的填充、对元素的属性进行编辑以及对元素进行选择，即可完成一个优美网页。 {84% : 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内容的排版，使网页错落有致，更加得体优雅。如同HTML一样，功能强大，使用简洁。Css通过定义一组组的属性，并将这些属性通过适当的语法作用在HTML文档中即可。 2.1.2 JavaScript和AJAX { 61% : JavaScript简称js，运行于浏览器中的解释性语言。 }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，{88% : 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。Js功能强大，但使用却并不复杂，通常有编程基础及经验的人几个小时即可入门，他的大多数语法如，循环，分支，函

数编写，对象编写等都与其他面向对象语言无二致，稍微注意一下原型链即可。{ 56% : JavaScript代码由一对＜script＞ ＜/script＞元素包含起来，}允许放到html文件内任何位置执行，也可以单独保存于一个后缀为.js的文件中，通过html适当的语法引入执行。 {82% : Ajax（Asynchronous JavaScript + XML）是一种设计模式。 }{ 59% : 过去的网页采用的是静态技术， }即使请求的网页只有细微的差别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而生，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，{ 68% : 核心是借助xmlhttprequest对象处理各部分细节。 }Ajax一般步骤为，{ 55% : 首先new一个xmlhttprequest对象， }然后编写回调函数（指ajax请求完成后执行的函数），再对发送的请求进行一些设置，比如是否附带数据，数据交互格式等等，最后将请求发出即可。 本软件的开发过程中，还用到了少量的Jquery。Jquery即js的一个第三方开发框架，它在js的基础上进行高一层的封装，将一些常用的操作封装成简约的符号，使开发者可以迅速找到要操作的DOM，其独创的链式写法，极大的精简了代码的结构。同时，它还优化了js的许多方法，并提供了更简洁的接口。Jquery的使用十分简单，{ 63% : 在HTML的head元素中，通过＜script src="https://code.}{ 63% : jquery.com/jquery-3.4.1. }{ 59% : min.js" > ＜/script＞引入后即可正常使用。 } 2.2 后端技术 2.2.1 后端框架 { 62% : 后端框架主要采用了flask框架技术，}flask即一种轻便的满足wsgi规范的python第三方开发框架，其中jinja2引擎可以渲染html模板，完成前后端分离，让前端人员可以集中注意力在精美界面的设计上，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，很大程度地提升了了web应用研发速度，简单易用而又不失强悍功能，是本系统主要后端技术。Flask虽然功能强大，但初步的使用并不困难，使用@app.route()指定处理的请求的URL及方法类型，紧随其后行跟一个def xxx()指定请求的处理函数，这样一次完整处理就完成了，简单而又层次分明。 2.2.1 python编程技术 { 61% : Python是本软件采用的最主要的语言，}它完成了本软件七成以上的工作量。Python由Guido van Rossum在圣诞节晚上消磨悠闲无趣的光阴所开发的解释性语。{ 56% : Python的出现，震撼了整个编程界， }它虽然与Java、c++等同属高级语言，但是基本数据结构抽象层次更高，这意味着它将对开发者更加的友善。{ 76% : 同时，python是弱类型语言， }解释器会根据变量内容自动地转变成合适的类型。{ 76% : Python是纯粹的面向对象编程语言，}python里，万物都是对象，因而可以python中的对象通常都会有一些方法，对开发者非常便利。它的另一大优点便是其模块化的结构方式，让调用第三方的模块变得方便简单，因此网上有许许多多的优秀的第三方功能模块可供使用。总之，python让开发人员从各种琐碎的细节之中抽离出来，集中精神在软件的设计与解决问题的思路上。综上，选用python最为本软件的主要开发工具无疑是非常明智的。 2.3 开源库 2.3.1 nmap与python-nmap { 78% : Nmap是一款开源的扫描工具, }用于系统管理员查看一个大型的网络有哪些主机及其上运行何种服务[9]。{ 59% : python-nmap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。{ 58% : Nmap模块是端口扫描与服务发现的中坚模块。 }Nmap使用方法比较简单，首先通过PortScanner()方法构造一个实例，端口、服务及版本等的扫描即可通过这个实例完成。Scan方法接收一些参数，用于指定IP、端口以及一些扫描设置。扫描完成

后，结果可通过调用这个对象的特定属性查看。 2.3.2 scapy Scapy为一个出色的TCP/IP协议包处理库，它能够方便的创建和发射协议包，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。Scapy模块通过xxx()/xxx()/string的形式构造数据包，其中，string为数据包携带的数据，xxx指明数据包的层次，如IP（）指定存在IP层。通过sr与sr1等方法即可完成数据包的发射，简单强悍。 2.3.3 request request是一个优秀的web服务处理库，request可以很方便的处理http数据包。它主要有get以及post两个函数，分别处理web服务中的get以及post提交方式，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。FTP模块主要有FTP()、connect()以及login()等函数及方法，分别负责创建ftp对象、连接ftp服务端口以及登录等操作，使用方便简单。 2.3.5 paramiko { 59% : 这个模块用于处理secure shell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。{ 58% : Ssh的使用并不复杂，首先通过SSHClient()创建一个ssh对象， }{92% : 然后使用set_missing_host_key_policy(paramiko. }{ 72% : AutoAddPolicy())方法初始化对象， }{ 69% : 而后使用Transport(ip, } port)方法连接对应的端口，{ 60% : 最后使用connect()方法登录。 } 2.4 端口扫描技术 端口扫描意为，一些非正常处理需要的人发送若干奇怪的数据包到目标计算机特定端口，意图了解计算机着些端口的相关信息。端口扫描结果可以了解到端口的开放信息，服务的开放情况等等。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 { 56% : 一个完整的tcp连接的建立历经三个过程： }首先，{ 63% : 客户端向服务端对应端口发送syn包， }清求建立连接；然后，服务端对应端口捕捉发送方的syn包之后，{ 57% : 发送一个syn ack包进行回复； }第三阶段，请求连接的一方再发送一个ack包到服务端进行确认。至此，连接已建立好。完全连接扫描即与服务端对应端口构造tcp连接，若可以构造连接表示端口处于开的状态，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syn ack包，则说明端口开放，返回一个rst包关闭连接；倘若发送过来的是一个rst包，意味着对应端口处于关状态，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。这种扫描相对于全连接扫描，{ 77% : 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扫描进行端口快速隐匿扫描。 2.5 服务发现技术 2.5.1 ftp服务发现 { 57% : ftp服务发现通过与指定端口建立tcp连接， }完成三次握手后，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，否则不存在ftp服务，遍历所有开放的tcp端口，即可测出系统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，{ 59% : 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）即向计算机任何组成部分逻辑上）或者运行于其上应用实施的任何类型的进攻动作，以毁坏或者盗取数据居多。Cyberattack种类繁多，数不胜数，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。 2.6.1 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。 2.6.2 dos攻击 Dos（拒绝服务）攻击是说，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，会在协议栈中分配出空间，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，有数量规模巨大syn包涌入服务端，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。 2.7 Linux技术 { 55% : Linux是一套免费使用和自由传播的类 Unix 操作系统， }是一个基于 POSIX 和 UNIX 的多用户、多任务、支持多线程和多 CPU 的操作系统[10]。Linux需要的硬件条件比较低，在虚拟机也能流畅运行，{ 55% : 基于这个原因本次测试环境选择了Linux系统， }测试环境的搭建主要用到了一些Linux基本操作。 2.8 涉及到的网络协议 网络扫描软件必然是离不开是离不开tcp/ip协议的，针对本软件的开发主要涉及协议，以下简要介绍一下： 2.8.1 tcp三次握手 { 55% : tcp三次握手：构造一个完整的tcp连接， }{ 55% : 历经三个过程，称为“三次握手”。 }开始时，请求连接方向服务端发送syn数据包申请建立连接；第二阶段，服务端获得刚才传输到的数据包后，回复一个syn ack包，表示允许请求，等待客户端回应；第三阶段请求连接方获取服务端回应的数据包后，{ 56% : 再发送一个ack包到服务端，表示确认连接。 }这时，一个完全的tcp握手过程完成，连接建立完毕。 2.8.2ftp协议 { 79% : ftp(File Transfer Protocol)，是互联网中最常用的文件传输协议。 }该协议访问机制采用交互性命令，客户端可以指定使用得文件类型和格式（比如是否使用ascii码），{ 57% : ftp隐藏了各种不同操作系统的细节， }因而适合在不同电脑中传送文件，{ 64% : ftp是基于tcp服务之上， }提供了文件上传下载等许多基础服务，因而其中的二进制流传输有保证的。ftp能减少甚至消除文件在不同电脑下的不兼容问题。ftp使用C/S架构，{ 57% : 一个服务端进程可服务若干客户进程。 }{ 55% : 一个完整的ftp服务器有两个主要模块：主进程， }完成客户进程的连接请求；还有一些子进程，负责为某一请求提供服务。主进程的工作原理： （1）打开约定

俗成的ftp端口（21），以便客户端连接。 （2）等待客户进程连接。 （3）运行附带进程为客户进程的连接提供服务，附带进程服务完成自动退出，其在处理时可能根据具体情况产生若干新的附带进程。 （4）重新处于等候状态，{ 67% : 继续服务不同客户进程发起的连接， }主进程与附带进程并行运行。 { 73% : ftp协议限定了控制协议传送与保存的多种方案， }从4个选择挑选其一： （1）文件格式：ASCII码等编码类型/ 图像视频等二进制文件/ 本地存储文件类别 （2）格式管理：本选项主要处理ASCII格式编码，打印选项为否(Default choice)/ 远程Login格式管理 （3）组织：文件结构(Default choice，文件在计算机中以字节流方式存在)/ 记录结构(For text files) （4）传输方式：流方式(Mode selection，文件采用字节流进行传送，针对文件结构，发送者在文件尾给出结束标记，针对记录结构，有特定的标记方式)/ 块方式(文件按照一块一块传输，每个块之前存在1个或若干个Header byte)/ 压缩方式 { 73% : ftp有两种工作模式，主动模式和被动模式[11]。 }两种说法是针对服务端来说的，{ 59% : 在传送数过程中，服务端先对客户端发起连接， }称为主动模式；否则请求服务方率先对服务器发起连接，称为被动模式。被动模式下，通常需要开放防火墙端口，以便客户端能够连接进来。 2.8.3 ssh协议 {84% : ssh全称Secure Shell， }ssh能加密传输的数据以抵御”中间人”攻击，{ 66% : 同时还可以杜绝Domain Name System欺骗， }加密数据必然带来性能上的损失，ssh的压缩传输技术可以极大的缓解这种损失，ssh可以给ftp生成一个安全的”传输隧道”。 { 73% : Ssh主要部分是三个协议：传输层协议，提供服务器认证、数据机密性以及信息完整性的支持； }{85% : 用户认证协议，为服务器鉴别客户端的身份； }{82% : 连接协议，将加密的的信息传输通道复用成多个逻辑上的通道，提供给更高层的应用协议使用。 } 像很多安全通讯协议一样，{ 61% : ssh存在一系列安全的密钥机制。 }它强制每个使用它的终端必须有一个密钥对，服务端验证客户端的密钥后，才能为其提供服务，单个主机能够接纳若干密钥，{ 58% : 对于不一样的密钥算法持有不一样的密钥， }要求必须存在由DSS生成的密钥。 Ssh协议工作过程包括五个过程： （1）版本号协商过程：此阶段协商通信双方使用的ssh协议版本，首先服务器开放22端口，以便接收客户进程的连接；{ 73% : 客户进程对服务器对应端口发送连接请求， }完成三次握手后，服务器给客户进程传输一个含有ssh协议版本信息的数据包；客户端收到包后，解析数据并且判断双方协议版本孰高孰低，低版本优先；判断完成后，发送一个决定报文，该报文包含采取的协议版本；{ 56% : 服务器获取客户进程发来的数据包后， }二次确认，是否能在该协议上工作，如果可以，则进入下一个过程，不然就切断会话。 （2）密钥和算法协商过程：通信双方互相传输一个存在支持的公钥算法集合、加密算法集合、MAC（消息验证码）算法集合、压缩算法集合等信息的数据包给彼此，双方根据自己及对方使用的算法决定采取何种算法；通信双方采取DH交换算法给出主机密钥对等信息，求出对话密钥以及对话 ID。 （3）认证过程：{ 72% : 客户进程向服务器发起认证请求， }请求中含有账号、认证方法以及密码等信息；服务端对客户端进行确认，返回成功消息或者包

含可重新认证的方法列表；一直循环上面的过程，除非认证成功或者次数封顶，服务器断开会话。 （4）会话请求过程：上面的认证阶段顺利完成后，客户进程对服务器申请会话连接；{82%：服务器响应客户端请求，若允许，则回复 SSH_SMSG_SUCCESS包，否则回应SSH_SMSG_FAILURE包。 } （5）此阶段，数据可以双向传输；客户端发送加密后的指令；服务端解密数据，处理客户端命令，返回相应数据；客户端对数据相应处理。 2.8.4 http协议 { 56%：http协议全称超文本传输协议，是web应用的基础，各种www文件均遵循这个协议。 }http协议为运行于tcp之上应用协议，由请求和响应组成，默认工作在80端口上。协议的数据格式类似，都是header+body的形式。 一次http叫做一次事务，运行流程如下： （1）用户在浏览器地址栏输入URL （2）浏览器解析URL并封装成http请求，发送出去 （3）服务端收到请求后，返回一个响应 （4）浏览器解析响应报文并进行渲染 这时，{ 64%：一次完整的通信就处理完毕了。 } http请求有很多种，{ 55%：用得多的请求就两种，get及post。 }{ 57%：get请求包含请求的url，即网址，以及查询字符串。 }查询字符串从’ ？’ 开始，以 ‘xxx’ =xxx形式，通过’ &’ 符号连接，get请求长度有限制，而且以明文展示在浏览器地址栏。{ 62%：Post请求与get请求类似， }但是post请求可以将请求参数放到body中，get请求body为空。 2.8.5WSGI规范 由于本软件采取python编写，web开发也是一个重要部分，因此，有必要介绍一下python 网站开发必须了解的规范WSGI规范。 {94%：WSGI全称Web Server Gateway Interface， }它并不是一个而具体的模块或者框架等，而是一个规范，本软件采用的flask框架就是基于WSGI规范的web开发框架。WSGI主要由两个部分构成，{ 71%：某个支持WSGI协议的服务器，一个application。 }服务器把接收到的socket数据包解析，将URL、查询字符串以及请求参数封装于environ中（environ属于哈希数据结构）并发送到app；同时，服务器还将名为start_response的回调方法发到appapplication，{ 58%：该方法需要两个参数，第一个为字符串， }第二个为一个字典，字典包含了响应头信息。{ 73%：App首先执行start_response， }该方法将参数封装成http协议头返回浏览器，接着执行开发者在app中自定义的操作，最后返回响应body，接下来服务器综合处理，将响应信息返回到客户端。至此，完整的http通信便完成了，WSGI是朴素的http通信的一次抽象，但是具体的开发很少会直接用这种方法，通常都是采用基于WSGI更高层的抽象，比如flask框架等。 2.9 正则表达式 { 60%：正则表达式是一种处理字符串的技术， }它给出了若干基本的符号及其意义，通过综合使用这些符号，得到一个字符串的匹配规则，这种规则定义了一种类型的字符串。通过正则表达式，可以很容易的自定义规则，从一个文本中找到想要的某些字符串。正则表达式具有灵活而用处广泛的特点，{ 60%：可以很简单的进行复杂的字符串操作， }这种技术将在服务发现时用到，将用来从banner中匹配出特点的服务信息。正则表达式在python中的运用很简单，首先通过导包引入re模块，然后通过re.{ 61%：match(str1,str2)， }第一个参数定义匹配规则，第二个参数为需要从中提取字符串的字符串。 3 需求分析 3.1输入输出需求 <p

style="margin:3px">软件需要对给定的IP地址和端口进行处理，{ 61%：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，一些存在的漏洞，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。{ 69%：本软件后端结构如图3.1所示： } 图 3.1后端模块图 （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，{ 56%：运行服务的软件信息以及软件的版本信息， }并返回浏览器端。 { 55%：（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。 （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，调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 界面采用ajax以及json与后台交互，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。软件是为人服务的，而前端是直接同使用者接触的部分，要求简单易用以及优美舒适。 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ftp、ssh以及web等服务以供测试。由于条件所限，不能使用多台计算机去协同演示，因此，测试环境与软件将并存于一个计算机之中，这就要求测试环境必须安装于虚拟机中，测试环境应当尽可能占用资源少，运行稳定。 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，因此本软件对性能要求颇高；同时，软件应当尽可能操作简单友好，界面美观优雅，以适应与人的交互。 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。同时，考虑到界面是直接与人进行交互的部分，还对界面的样式进行了一定的处理，插入了一些优美而切题的图画，以及做了一些等待时的动画效果。 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，服务软件鉴别与版本发现等。扫描模块下共有：tcp_scan模块、ftp模块、web模块、ssh模块，负责具体功能的实现，如图4.2： 图4.2 扫描模块结构 Tcp_scan模块完成tcp端口开放情况扫描，ftp模块完成ftp服务发现功能，ssh模块完成ssh服务发现功能，web模块完成web服务发现功能。 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4.3所示： 图4.3 评估模块 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 整体设计 { 62% : 系统各个模块的设计如上所述， }他们关系如图4.5： 图4.5 整体设计 5 系统实现 5.1 概述 用户面对前端界面，输入IP与端口信息，{ 61% : 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。 5.2 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函数发送数据包并接受一个回应包，对回应包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；{ 56% : 倘若收到的是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5.2： 图5.2 端口扫描流程 5.3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，{ 60% : 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相关方法，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，不然没有ftp服务。关键代码如图5.3.1： 图5.3.1 ftp服务发现 5.3.2 ssh服务发现 ssh服务封装于ssh模块，{ 60% : 该模块需要的输入参数为：ip(目标IP)， }port(要检测的所有端口)。通过与目标端口进行会话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，从而判断是不是存在ssh service。{ 55% : 关键代码如图5.3.2所示： } 图5.3.2 ssh服务发现 5.3.3 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，{ 55% : 关键代码如图5.3.3所示： } 图5.3.3 web服务发现 5.4 模拟攻击 5.4.1 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，各函数具体实现如图5.4.1： gen_syn(toal，dst_ip)如图5.4.1（1）： 图5.4.1（1）

gen_syn函数 send_pkt(pkt_num,dst_ip)，如图5.4.1（2）: 图5.4.1（2）send_pkt函数 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，syn_flood(num,total,dst_ip)，如图5.4.1（3）： 图5.4.1（3）syn_flood函数 5.4.2 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，{ 61% : 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，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，{ 63% : 当为true时退出，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，关键代码如图5.4.2(1)(2) (3) (4)： 图5.4.2 （1）ftp暴力破解 图5.4.2 （2）ftp暴力破解 图5.4.2 （3）ftp暴力破解 图5.4.2 （4）ftp暴力破解 （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，关键代码如图5.4.2（1）、5.4.2（2）以及5.4.2（3）： 图5.4.2（1）ssh暴力破解 图5.4.2（2）ssh暴力破解 图5.4.2（3）ssh暴力破解 5.5 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，{ 59% : 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。{ 59% : 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；{ 59% : 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，界面的运行流程如图5.5： 图5.5 前端界面示意图 5.6 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） 处理界面请求：当用户输入URL请求界面时，使用Flask模块构造处理函数，返回模板中的html网页并进行一些初始化工作，如图5.6（1）： 图5.6（1） 处理界面请求 （2）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，{ 55% : 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，关键代码如图5.6（2）、5.6（3）以

及5.6（4）： 图5.6（2）处理扫描请求 图5.6（3）处理扫描请求 图5.6（4）处理扫描请求 （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，如图5.4（5）： 图5.4（5）处理ftp与ssh爆破测试 （2）处理dos攻击测试，类似地，调用syn_flood函数即可，如图5.4（6）： 图5.4（6）处理dos攻击测试 5.7 测试环境 { 55% : 首先需要安装VMware虚拟机，}安装VMware比较简单，一路回车即可，{ 56% : 下面主要介绍一下安装kali linux以及服务的搭建。 } 5.7.1 安装kali linux { 70% : Kali linux是linux的一个发行版， }{ 59% : 首先打开VMware虚拟机： } { 67% : （1）选择创建虚拟机，选择自定义，然后点下一步； } { 57% : （2）选择kali linux的路径； } （3）选择客户机操作系统，这里勾选Linux即可； （4）配置系统的内存，这里选400M，磁盘大小50G； （5）开机，进行安装； （6）进入安装界面，{ 73% : 选择图形界面安装（Graphical install）； } （7）选择使用整个硬盘； （8）将所有文件放在同一个分区中； （9）设置密码； （10）将GRUB安装至硬盘； （11）安装完成，输入账户名密码即可进入。 Kali linux到此就安装完成了，{ 56% : 接下来在系统中搭建各种服务。 }为了能更方面的使用kali linux的包管理系统进行安装，这里首先得更新一下源列表，使用国内的镜像，{ 78% : 使用sudo vim /etc/apt/sources. }list命令打开配置文件，将中科大的源地址写入文件中即可，如下图5.7.1所示： 图5.7.1 源配置 5.7.2 搭建ftp服务 首先安装ftp服务软件vsftpd，{ 65% : 使用包管理命令直接安装即可，输入命令sudo apt-get install vsftpd安装即可， }安装好软件之后需要进行简单的配置一下，{ 60% : 使用命令vim/etc/vsftpd. }conf打开配置文件，将配置文件配置成如下图5.7.2所示： 图5.7.2 ftp配置文件 新建一个名为uftp的用户 sudo useradd -d /home/uftp/ -s /bin/bash uftp；为用户设置密码，sudo passwd uftp，此时ftp服务基本已经搭建完毕。 5.7.3 搭建ssh服务 { 59% : Kali linux默认没有安装ssh服务，需要手动安

装， }类似地，{ 55% : 使用命令apt-get install openssh-server， }将ssh服务配置为开机启动，以免每次都要手动开启， { 64% : （1）修改ssh_config文件。 }{93% : 命令：vim /etc/ssh/sshd_config； } {95% : （2）将#PasswordAuthentication no的注释去掉， }并且将NO修改为YES； （3）将#PermitRootLogin yes的注释去掉 //我的kali中默认去掉了注释； （4）启动SSH服务，命令为：/etc/init.d/ssh start // 或者service ssh start； { 55% :（5）验证SSH服务状态，命令为：/etc/init.d/ssh status； } （6）添加开机自启动 update-rc.d ssh enable。 默认情况下，{ 58% : linux不允许使用root管理员账户远程登录，得修改一下配置，使用命令vim /etc/ssh/sshd_config打开配置文件，把PermitRootLogin设置为yes即可， }此时，ssh服务就搭建好了。 5.7.4 搭建web服务 Web服务采用dvwa靶场，需要安装apache、mysql以及php 安装apache，{80% : 使用包管理命令安装即可，sudo apt-get install apache2， }将apache2设置为开机启动，/etc/init.{ 57% : d/apache2 status。 } { 67% :（1）安装MYSQL数据库，sudo apt-get install mysql，将mysql设置为开机启动，/etc/init. }d/mysql status； （2）安装PHP，{86% : sudo apt-get install php5， }安装过程中会有问题，一路回车即可，同样的，设为开机启动，不在赘述 （3）配置dvwa靶场，首先去github下载好dvwa安装包，然后将下载好的安装包解压并改名为dvwa，复制到/var/www/html 文件夹中； { 57% :（4）将apache2停止：service apache2 stop； } （5）给dvwa文件夹相应的权限：chmod -R 755 /var/www/html/dvwa； （6）打开mysql： mysql -u root -p； （7）打开mysql： mysql -u root -p； （8）创建数据库：create database dvwa;； { 62% :（9）启动apache2服务：service apache2 start； } { 70% : 然后终端执行mysql -u -root -p,回车后输入密码， }执行以下SQL语句： create user 'dvwauser'@'localhost' IDENTIFIED BY ''; GRANT ALL PRIVILEGES ON *.* to 'dvwauser'@'localhost'; flush privileges quit 修改dvwa的配置文件，cd /var/www/html/dvwa/config/ vi config.inc.php.dist config.inc.php

将$_DVWA['db_user'] = 'root'；修改为：$_DVWA['db_user'] = 'dvwauser'; 将$_DVWA['db_password'] = 'p@ssword'；修改为： $_DVWA['db_password'] = '' ； 这样dvwa靶场就配置好了，可在浏览器输入linux的主机地址即可访问到，至此，整个web服务就搭建好了。 6 系统测试 6.1 扫描功能 为了测试扫描功能的完整性，做以下处理，如表6-1-1所示： 表6-1-1 扫描功能测试表 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，如表6-1-2： 表6-1-2 非法输入时的扫描功能测试表 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 6.2 ftp爆破测试 测试ftp爆破功能如表6-2-1： 表6-2-1 ftp爆破测试表 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 显示爆破解果及一些加固建议 测试异常情况下的ftp爆破功能如表6-2-2： 表6-2-2 ftp爆破测试表 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 测试超时情况下的ftp爆破如表6-2-3： 表6-2-3 ftp爆破测试表 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 6.3 ssh爆破测试 测试ssh爆破功能如表6-3-1： 表6-3-1 ssh爆破测试表 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加固建议 测试异常情况下的ftp爆破功能如表6-3-2： 表6-3-2 ssh爆破测试表 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 测试超时情况下的ftp爆破功能如表6-3-2： 表6-3-3 ssh爆破测试表 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 6.4 dos攻击测试 测试dos攻击如表6-4-1： 表6-4-1 dos攻击测试 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 测试非法输入时如表6-4-2： 表6-4-2 dos攻击测试 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 6.5 测试结果分析 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[12]；对于一些不符合预期的情况，已改进使其能正常工作。 7 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。 7.1 感想与收获 三个月前，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，{ 65%：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

一下前人是怎么完成这个任务的，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，{ 57% : 对调试错误有了更深层次的认识。 }{ 57% : 调试bug是软件开发一个重要的必经过程， }虽然大家都不想经历，但通常它都会占据总开发接近一半的时间。整个毕设做下来，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，对学习也有了新的认识。{ 57% : 学习其实是一个积累与思考的过程，学习一个东西，{ 56% : 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。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！ 7.2 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，{ 64% : 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。{ 56% : 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。{ 56% : 同时，本软件由于采用B/S架构，只需在浏览器中即可运行，具有使用极其便捷的优点。 然技术与知识所限，软件的不足也很明显。{ 76% : 网络扫描是一把双刃剑，用得好，就是提升系统安全的利器，{

56% : 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，{ 63% : 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；{ 56% : 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。{ 63% : 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。{95% : 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。{100% : 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，{ 57% : 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研究生亚历珊卓·艾尔巴金与其大作，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。{99% : 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，{81% : 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。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，{ 77% : 在此谨向理查德·斯托曼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！ 参考文献 [1] 李志勇,葛先军，刘锋.网络扫描技术分析[J].海军航空工程学院学报,2005, 20(5):588~590. [2] 李瑞民.网络扫描技术揭秘：原理、实践及扫描器的实现[M].北京:机械工业出版社,2010：100-500. [3] (美)Wesley J.chun.Python核心编程(第二版)[M].北京:人民邮电出版社,2008：12-100. [4] 李文江.浅谈网络扫描技术在网络安全方面的应用[J].数字技术与应

用,2016(3):215-225. [5] 张友旭.分布式隐匿网络扫描关键技术研究[D].哈尔滨：哈尔滨工程大学,2016. [6] 王勇.关于计算机网络安全与漏洞扫描技术的分析探讨[J].数字技术与应用,2016：10~12. [7] Stanley B. Lippman,Josée Lajoie,Barbara E. Moo. C++ Primer（中文版 第5版）[M].北京:电子工业出版社,2013：50-120. [8] Kevin R. Fall.TCP/IP协议详解卷一：协议（原书第二版）（吴英）[M].北京:机械工业出版社,2016:80-200. [9] 魏锦慧.用于Nmap的攻击工具集的设计与实现[D].长春：吉林大学,2006. [10] 郭帅强.社交网络中的个人隐私安全保护问题研究[D].广州：广东财经大学,2016. [11] 韦超.基于SSL协议的FTP服务器设计与实现[D].北京：中国地质大学,2016. [12] 李新华.基于虚拟化的网络演练竞技平台的设计与实现[D].北京：北京邮电大学,2017. [13] 杨振.基于Linux的抗DDoS防火墙的设计与实现[D].天津：天津大学，2007
</br>
</br> <h5>检测报告由PaperTime文献相似度检测系统生成</h5> </body> </html>