PaperPP检测报告简明打印版

总文字复制比：24.55%
去引用复制比：24.55%
编　号：N44FO9L3AYXRMDF0J08ZDVUB6QQ7L4H5
标　题：1651200111
作　者：网络扫描器毕业论文
长　度：15,587字符
时　间：2020-05-06 17:14:01
比对库：中国学位论文全文数据库；中国学术杂志数据库；中国重要会议论文全文数据库；英文论文全文数据库；互联网资源；自建比对库

相似资源列表(学术杂志，本科论文，硕博论文等本地数据库资源)
1. 相似度：1.78%　标题：《基于VC++平台的远程主机操作系统探测技术的应用与开发》
类型：学术杂志　年份：2015　作者：赵 宏
2. 相似度：0.71%　标题：《局域网环境下若干安全问题及对策》
类型：本科论文　年份：2009　作者：李玲
3. 相似度：0.71%　标题：《局域网环境下若干安全问题及对策》
类型：本科论文　年份：2006　作者：佚名
4. 相似度：0.52%　标题：《网络基础与osi参考模型issue1.0》
类型：硕博论文　年份：2007　作者：佚名
5. 相似度：0.48%　标题：《以太网交换机基础培训教材》
类型：硕博论文　年份：2003　作者：佚名
6. 相似度：0.36%　标题：《浅析网络安全扫描技术》
类型：学术杂志　年份：2006　作者：佚名
7. 相似度：0.35%　标题：《基于ASP.NET的实验室开放管理系统设计与实现》
类型：硕博论文　年份：2015　作者：佚名
8. 相似度：0.34%　标题：《区域交通控制系统的设计与实现》
类型：硕博论文　年份：2017　作者：佚名
9. 相似度：0.33%　标题：《基于hadoop的属性加密系统》
类型：硕博论文　年份：2015　作者：佚名
10. 相似度：0.33%　标题：《基于GIS下的城市规划管理系统的设计与实现》
类型：硕博论文　年份：2016　作者：佚名
11. 相似度：0.32%　标题：《网络安全扫描系统的设计与实现》
类型：硕博论文　年份：2017　作者：佚名
12. 相似度：0.30%　标题：《企业网络资源管理系统》
类型：硕博论文　年份：2012　作者：佚名
13. 相似度：0.30%　标题：《SDN安全态势评估系统》
类型：硕博论文　年份：2014　作者：佚名
14. 相似度：0.29%　标题：《顶点着色算法解决考试冲突问题的研究与实现》
类型：硕博论文　年份：2012　作者：王五,
15. 相似度：0.28%　标题：《基于网络的漏洞器》
类型：本科论文　年份：2008　作者：佚名
16. 相似度：0.27%　标题：《烟草配送中基于android的车载gis终端设计与实现》
类型：硕博论文　年份：2017　作者：佚名
17. 相似度：0.27%　标题：《基于用电信息采集的线损管理系统设计与实现》
类型：硕博论文　年份：2017　作者：佚名
18. 相似度：0.26%　标题：《基于微信的图片打印分享平台》
类型：硕博论文　年份：2016　作者：佚名
19. 相似度：0.26%　标题：《基于RFID智能高清卡口在交通管理层面的设计与实现》
类型：硕博论文　年份：1998　作者：佚名
20. 相似度：0.26%　标题：《基于J2EE的网上银行系统的设计与实现》

类型：硕博论文 年份：2016 作者：佚名
21. 相似度：0.26% 标题：《基于mapreduce的分布式web漏洞扫描系统的研究与设计》
类型：硕博论文 年份：2017 作者：佚名
22. 相似度：0.26% 标题：《高性能采集软件关键技术研究和实现》
类型：硕博论文 年份：2017 作者：佚名
23. 相似度：0.26% 标题：《delphi论文企业生产计划管理系统论文》
类型：本科论文 年份：2004 作者：佚名
24. 相似度：0.26% 标题：《delphi论文生产管理系统论文》
类型：本科论文 年份：2004 作者：佚名
25. 相似度：0.26% 标题：《密集wlan中高效接入算法研究》
类型：硕博论文 年份：2017 作者：佚名
26. 相似度：0.25% 标题：《基于分布式计算模式的视频处理框架设计及优化》
类型：硕博论文 年份：2007 作者：佚名
27. 相似度：0.25% 标题：《基于IOCP结构的P2P节点选择与分割混合模型的研究》
类型：硕博论文 年份：2015 作者：吴金辉
28. 相似度：0.25% 标题：《面向容器化应用的资源管理系统》
类型：硕博论文 年份：2016 作者：佚名
29. 相似度：0.24% 标题：《SuperScan端口实验》
类型：学术杂志 年份：2010 作者：佚名
30. 相似度：0.23% 标题：《浅析网络安全扫描技术》
类型：学术杂志 年份：2011 作者：赵妙军
31. 相似度：0.23% 标题：《基于hadoop平台的图书馆读者兴趣分析与导向系统模型的建立》
类型：硕博论文 年份：2017 作者：佚名
32. 相似度：0.23% 标题：《浅析网络安全扫描技术》
类型：学术杂志 年份：2010 作者：赵妙军
33. 相似度：0.21% 标题：《《CCNA学习指南第6版640-802》Word中文版》
类型：硕博论文 年份：2002 作者：佚名
34. 相似度：0.21% 标题：《实验2网络及安全评估实验》
类型：本科论文 年份：2010 作者：佚名
35. 相似度：0.20% 标题：《基于SIP和ICE的VoIP系统的NAT穿透研究》
类型：硕博论文 年份：2016 作者：吴新生
36. 相似度：0.19% 标题：《第二部分SWITCH笔记》
类型：本科论文 年份：2008 作者：佚名
37. 相似度：0.19% 标题：《面向数据中心网络的SDN控制器设计与实现》
类型：硕博论文 年份：2017 作者：佚名
38. 相似度：0.18% 标题：《计算机网络实验网络实验报告》
类型：本科论文 年份：2011 作者：佚名
39. 相似度：0.18% 标题：《一种用户可扩展的网络发包器的研究》
类型：硕博论文 年份：2017 作者：佚名
40. 相似度：0.17% 标题：《中石化资金集中管理系统设计与实现》
类型：硕博论文 年份：2017 作者：NVARCHAR(30)
41. 相似度：0.17% 标题：《局域网环境下若干安全问题及对策》
类型：本科论文 年份：2011 作者：李玲
42. 相似度：0.16% 标题：《网络安全论文-ARP欺骗原理及防御手段》
类型：本科论文 年份：2016 作者：佚名
43. 相似度：0.15% 标题：《城域网光纤传输网络规划与设计》
类型：本科论文 年份：2014 作者：佚名
44. 相似度：0.14% 标题：《基于FPGA的万兆以太网数据分发平台设计》
类型：硕博论文 年份：2016 作者：佚名
45. 相似度：0.14% 标题：《ARP病毒》
类型：学术杂志 年份：2009 作者：佚名
46. 相似度：0.13% 标题：《广电媒体资源管理系统的设计与实现》
类型：硕博论文 年份：2015 作者：:果思
47. 相似度：0.13% 标题：《广电媒体资源管理系统的设计与实现》
类型：硕博论文 年份：2015 作者：:果思

48. 相似度：0.12% 标题：《12kv变电站的数据采集与监视控制系统(scada)的研究》
类型：硕博论文 年份：2017 作者：REJEPOVA
49. 相似度：0.12% 标题：《计算机专业毕业论文答辩开场白范文》
类型：学术杂志 年份：2006 作者：佚名
50. 相似度：0.12% 标题：《数字测高仪数据处理与频高图参数度量系统设计》
类型：硕博论文 年份：2016 作者：佚名
51. 相似度：0.11% 标题：《Excel与VBA程序设计》
类型：硕博论文 年份：2005 作者：Mar
52. 相似度：0.09% 标题：《基于postgresql存储引擎多线程化的分析与实现base...》
类型：硕博论文 年份：2012 作者：佚名
53. 相似度：0.09% 标题：《基于nfv的安全服务系统与应用研究》
类型：硕博论文 年份：2017 作者：佚名
54. 相似度：0.07% 标题：《网络安全扫描的网络信息安全》
类型：学术杂志 年份：2006 作者：佚名
55. 相似度：0.07% 标题：《Dances with Wolves domestic fi...》
类型：学术杂志 年份：2006 作者：unknown
56. 相似度：0.07% 标题：《SQL注入攻击及防御研究》
类型：硕博论文 年份：2015 作者：:田玉
57. 相似度：0.07% 标题：《Analysis on the Software Proje...》
类型：学术杂志 年份：2010 作者：unknown
58. 相似度：0.06% 标题：《Regional power grid supporting...》
类型：学术杂志 年份：2006 作者：unknown
59. 相似度：0.05% 标题：《微信营销促进A旅游公司发展研究》
类型：学术杂志 年份：2009 作者：佚名
60. 相似度：0.05% 标题：《微信营销促进A旅游公司发展研究》
类型：学术杂志 年份：2016 作者：陈赛楠
61. 相似度：0.04% 标题：《网络安全漏洞的检测工具AccessDiver》
类型：本科论文 年份：2010 作者：林宏坡
62. 相似度：0.04% 标题：《计算机网络安全扫描技术研究》
类型：学术杂志 年份：2016 作者：易永红
63. 相似度：0.04% 标题：《网络安全漏洞的检测工具AccessDiver》
类型：本科论文 年份：2007 作者：佚名
64. 相似度：0.04% 标题：《网络安全漏洞的检测工具AccessDiver》
类型：本科论文 年份：2011 作者：林宏坡
65. 相似度：0.03% 标题：《基于微信公众平台的场馆微课程设计与开发》
类型：硕博论文 年份：2019 作者：李曼
66. 相似度：0.03% 标题：《发射_接收模块测试系统硬件设计与测试实现》
类型：硕博论文 年份：2017 作者：佚名
67. 相似度：0.03% 标题：《基于数据挖掘的Web用户使用模式生成方法研究》
类型：硕博论文 年份：2017 作者：张駿温

相似资源列表(道客巴巴，豆丁网，百度文库等云论文资源)

1. 相似度：2.94% 标题：《漏洞扫描技术_图文》
来源：https://wenku.baidu.com/view/1b24ba9d77c66137ee06eff9aef8941ea66e4b38.html
2. 相似度：2.00% 标题：《一种基于TCP / IP协议栈的操作系统识别技术》
来源：http://www.doc88.com/p-8728618530845.html
3. 相似度：1.39% 标题：《网络对抗3-攻击引言扫描监听(可编）》
来源：http://www.doc88.com/p-9794464804213.html
4. 相似度：1.22% 标题：《毕业设计(论文)说明书统一格式的规定》
来源：https://wenku.baidu.com/view/d3a5c5a758fb770bf68a556b.html?re=view
5. 相似度：1.22% 标题：《毕业设计(论文)说明书-详细》
来源：http://www.doc88.com/p-1886392319952.html
6. 相似度：1.15% 标题：《一种基于tcpip协议栈的操作系统识别技术》
来源：https://www.docin.com/p-1264826177.html
7. 相似度：0.82% 标题：《网络入侵与攻击 - 北京大学计算机系信息安全研究室》

来源：http://www.doc88.com/p-7465213975655.html
8. 相似度：0.74% 标题：《浅谈操作系统指纹识别》
来源：http://www.doc88.com/p-9837408052026.html
9. 相似度：0.71% 标题：《网络漏洞扫描技术【PPT】》
来源：http://www.doc88.com/p-7019532029865.html
10. 相似度：0.56% 标题：《网络安全攻防对抗实验》
来源：https://www.docin.com/p-350658139.html
11. 相似度：0.54% 标题：《基于51单片机的打地鼠实训报告》
来源：https://www.docin.com/p-1675652912.html
12. 相似度：0.40% 标题：《第5章漏洞检测_图文》
来源：https://wenku.baidu.com/view/c33111fd7d192279168884868762caaedd33ba1e.html
13. 相似度：0.34% 标题：《缓冲区溢出漏洞的静态检测及动态防护方法研究和实现》
来源：https://www.docin.com/p-748356824.html
14. 相似度：0.33% 标题：《（计算机应用技术专业论文）基于web的安全测评技术研究》
来源：https://www.docin.com/p-743871058.html
15. 相似度：0.32% 标题：《《操作系统》习题解答习题1 术语解释裸机 虚拟机 操作系统 ...》
来源：https://www.docin.com/touch_new/preview_new.do?id=938729617
16. 相似度：0.31% 标题：《Web应用安全之常见威胁》
来源：http://www.doc88.com/p-1146394346864.html
17. 相似度：0.31% 标题：《中级网络工程师2017下半年上午考试试题》
来源：http://www.doc88.com/p-3572525390296.html
18. 相似度：0.30% 标题：《计算机网络扫描技术的隐蔽性研究》
来源：http://www.doc88.com/p-1876944116483.html
19. 相似度：0.30% 标题：《端口扫描与系统漏洞检测.ppt》
来源：https://www.taodocs.com/p-157697912.html
20. 相似度：0.28% 标题：《C++程序设计与应用开发》
来源：http://www.doc88.com/p-1931694778652.html
21. 相似度：0.27% 标题：《多功能SQL注入检测系统的实现及攻击防范方法研究》
来源：https://wenku.baidu.com/view/55b5d8323968011ca3009180.html
22. 相似度：0.26% 标题：《北京交通大学通信工程综合实验_图文》
来源：https://wenku.baidu.com/view/866686a0f4335a8102d276a20029bd64793e625e.html
23. 相似度：0.26% 标题：《电力电子技术CAI仿真软件の研究开发》
来源：https://www.docin.com/p-1147592637.html
24. 相似度：0.26% 标题：《第11章 Python第三方库纵览》
来源：http://www.doc88.com/p-1196401689605.html
25. 相似度：0.26% 标题：《网络与信息攻击与防护》
来源：https://www.docin.com/p-305439804.html
26. 相似度：0.24% 标题：《对计算机网络信息安全及防护策略的研究.pdf》
来源：https://www.taodocs.com/p-19959913.html
27. 相似度：0.24% 标题：《EXCEL函数应用方法大全1》
来源：https://www.docin.com/p-946307913.html
28. 相似度：0.23% 标题：《移动应用开发复习》
来源：https://www.docin.com/p-1204817055.html
29. 相似度：0.23% 标题：《计算机网络安全--第六章 网络漏洞扫描技术.ppt》
来源：https://www.docin.com/p-463866328.html
30. 相似度：0.23% 标题：《计算机网络实验指导书2014.doc》
来源：http://www.doc88.com/p-4337076305943.html
31. 相似度：0.23% 标题：《网络漏洞扫描技术》
来源：https://wenku.baidu.com/view/0990d5174431b90d6c85c794.html
32. 相似度：0.22% 标题：《计算机网络实验指导书2013》
来源：https://www.docin.com/p-1823383855.html
33. 相似度：0.22% 标题：《计算机网络实验指导书2014》
来源：https://www.docin.com/p-1626155173.html
34. 相似度：0.21% 标题：《最美家庭事迹材料范文（共15篇）》
来源：https://www.docin.com/p-2123106885.html

35. 相似度：0.21% 标题：《JavaScript完全教程_图文》
来源：https://wenku.baidu.com/view/b2c9c6639fc3d5bbfd0a79563c1ec5da51e2d620.html
36. 相似度：0.21% 标题：《第6章_进程管理与作业管理1._图文》
来源：https://wenku.baidu.com/view/542e289e9fc3d5bbfd0a79563c1ec5da50e2d6d5.html
37. 相似度：0.21% 标题：《网络攻击实现技术研究》
来源：https://www.docin.com/p-1402415851.html
38. 相似度：0.21% 标题：《网络通信安全管理员(中级)-07-网络设备安全》
来源：https://www.docin.com/p-380757307.html
39. 相似度：0.21% 标题：《字符串 格式化 正则表达式》
来源：https://wenku.baidu.com/view/1127101891c69ec3d5bbfd0a79563c1ec5dad7e9.html
40. 相似度：0.21% 标题：《Linux网络编程第二版》
来源：https://wenku.baidu.com/view/2b31291fcf84b9d528ea7a7b.html
41. 相似度：0.21% 标题：《最美家庭事迹材料范文（共15篇）》
来源：https://www.docin.com/p-2108380942.html
42. 相似度：0.20% 标题：《信息管理学教程课后习题答案》
来源：http://www.doc88.com/p-8408527564465.html
43. 相似度：0.20% 标题：《信息管理学答案》
来源：http://www.doc88.com/p-3317470675940.html
44. 相似度：0.20% 标题：《计算机网络面试题(全)》
来源：https://wenku.baidu.com/view/445a3350915f804d2a16c114.html
45. 相似度：0.19% 标题：《毕业设计（论文）-基于C语言的端口扫描的实现》
来源：https://www.docin.com/p-919753359.html
46. 相似度：0.19% 标题：《网络对抗信息收集技术的研究》
来源：https://www.docin.com/p-1163600586.html
47. 相似度：0.18% 标题：《主机信息探测实验》
来源：https://www.docin.com/p-1815759837.html
48. 相似度：0.18% 标题：《单片机与以太网接口设计完整版》
来源：http://www.doc88.com/p-7836414279246.html
49. 相似度：0.17% 标题：《TCP_IP协议安全漏洞》
来源：https://wenku.baidu.com/view/f62d588b84868762caaed55d.html
50. 相似度：0.17% 标题：《TCPIP协议安全漏洞》
来源：https://wenku.baidu.com/view/38a2e64b0a1c59eef8c75fbfc77da26925c596e6.html
51. 相似度：0.17% 标题：《计算机通信毕业论文范文》
来源：http://www.docin.com/p-1332454503.html
52. 相似度：0.17% 标题：《网络安全及其对国际关系的影响¯以“斯诺登事件”为例》
来源：http://www.doc88.com/p-9909657586724.html
53. 相似度：0.17% 标题：《TCPIP协议安全漏洞》
来源：https://www.docin.com/p-1644868034.html
54. 相似度：0.17% 标题：《计算机通信毕业论文范文》
来源：https://www.docin.com/p-1332454503.html
55. 相似度：0.16% 标题：《网络信息安全防护策略(5篇)(共17724字)》
来源：http://www.doc88.com/p-7106387390901.html
56. 相似度：0.16% 标题：《TCP IP协议的安全性与防范论文》
来源：https://www.docin.com/p-301532219.html
57. 相似度：0.16% 标题：《2016计算机网络基础离线作业》
来源：https://wenku.baidu.com/view/50337a37b8f67c1cfbd6b8bd.html
58. 相似度：0.16% 标题：《iris抓包工具使用详解》
来源：http://www.doc88.com/p-3324680357063.html
59. 相似度：0.16% 标题：《Iris抓包对象应用详解[整理版]》
来源：https://www.docin.com/p-1225286419.html
60. 相似度：0.15% 标题：《试验三协议分析软件的使用》
来源：https://wenku.baidu.com/view/6c4e6ddbce84b9d528ea81c758f5f61fb73628b6.html
61. 相似度：0.14% 标题：《建筑施工风险管理预警系统的研究》
来源：https://www.docin.com/p-2107217884.html
62. 相似度：0.14% 标题：《建筑施工风险管理预警系统研究》

来源：https://www.docin.com/p-440937996.html
63. 相似度：0.12% 标题：《PRISMS: An Integrated, Open》
来源：https://link.springer.com/article/10.1007/s11837-018-3079-6
64. 相似度：0.12% 标题：《计算机网络中端口扫描技术初步探微》
来源：http://www.doc88.com/p-0018679497696.html
65. 相似度：0.12% 标题：《报文分析,技术介绍,ospf的报文格式,报文类型及含义》
来源：http://www.doc88.com/p-7973311532781.html
66. 相似度：0.12% 标题：《测绘程序设计vb》
来源：https://www.docin.com/p-1828975365.html
67. 相似度：0.12% 标题：《第10章安全脆弱性分析_图文》
来源：https://wenku.baidu.com/view/b13eee154973f242336c1eb91a37f111f1850dd0.html
68. 相似度：0.12% 标题：《第7章嵌入式系统网络接口(52)》
来源：https://www.docin.com/p-1301171716.html
69. 相似度：0.12% 标题：《网络攻防复习四川大学》
来源：http://www.doc88.com/p-1778988987938.html
70. 相似度：0.12% 标题：《第10章安全脆弱性分析_图文》
来源：https://wenku.baidu.com/view/0841d51350ea551810a6f524ccbff121dd36c52c.html
71. 相似度：0.11% 标题：《信息搜集》
来源：https://wenku.baidu.com/view/6275dc8516fc700abb68fcd2.html
72. 相似度：0.11% 标题：《ARM9嵌入式系统的设计基础教程 第7至13章 课件_图文》
来源：https://wenku.baidu.com/view/777c3bb368eae009581b6bd97f1922791788be34.html
73. 相似度：0.11% 标题：《Intelligent Monitoring System ...》
来源：http://www.doc88.com/p-2724838055707.html
74. 相似度：0.10% 标题：《计算机网络病毒防治技术分析》
来源：http://www.doc88.com/p-3837664103701.html
75. 相似度：0.10% 标题：《A comprehensive review on hybr...》
来源：https://link.springer.com/article/10.1007/s40534-019-0184-3
76. 相似度：0.10% 标题：《A survey of multidisciplinary ...》
来源：https://link.springer.com/article/10.1007/s00158-011-0701-4/fulltext.html
77. 相似度：0.07% 标题：《Logistics automation managemen...》
来源：http://www.doc88.com/p-6512593149877.html
78. 相似度：0.05% 标题：《Louvain-la-Neuve》
来源：https://wenku.baidu.com/view/63b83582d4d8d15abe234eb8.html

相似资源列表(百度知道，百度百科，博客等互联网资源)

1. 相似度：1.39% 标题：《2019年网络安全事件回顾》
来源：https://www.77169.net/html/250173.html
2. 相似度：1.39% 标题：《2019年网络安全事件回顾（国际篇）》
来源：https://netsecurity.51cto.com/art/202001/609166.htm
3. 相似度：1.39% 标题：《2019年30件国际网络安全大事件，你都知道吗？》
来源：http://iapp.hongjingedu.com/wap/news/show_198.html
4. 相似度：0.94% 标题：《同时多线程是什么是什么》
来源：https://developer.aliyun.com/askzt/4607409.html
5. 相似度：0.84% 标题：《多线程和mysql》
来源：https://blog.csdn.net/weixin_41922887/article/details/82792816
6. 相似度：0.83% 标题：《【计算机网络实验的软件】》
来源：https://www.csdn.net/gather_27/MtTacg1sODg4Ny1ibG9n.html
7. 相似度：0.78% 标题：《如何使用nmap入侵局域网的监控器》
来源：https://bbs.csdn.net/topics/392723947
8. 相似度：0.68% 标题：《【软件测试的目的和意义】》
来源：https://www.csdn.net/gather_28/MtTagg3sOTA0Ni1ibG9n.html
9. 相似度：0.68% 标题：《软件测试中的目的是什么意思 软件测试的目的是什么》
来源：http://www.51sjk.com/b1b94741/
10. 相似度：0.67% 标题：《第13章软件技术基础》
来源：https://ishare.iask.sina.com.cn/f/ouzif0tn71.html

11. 相似度：0.50% 标题：《渗透测试中信息收集的那些事》
来源：https://www.cnblogs.com/OpenCyberSec/p/10794124.html
12. 相似度：0.50% 标题：《渗透测试中信息收集的那些事 | 码农网》
来源：https://www.codercto.com/a/73125.html
13. 相似度：0.50% 标题：《渗透测试中信息收集的那些事》
来源：https://www.sohu.com/a/310913009_354899
14. 相似度：0.39% 标题：《渗透测试之信息搜集》
来源：https://segmentfault.com/a/1190000015895031
15. 相似度：0.35% 标题：《软件测试目的和作用》
来源：https://blog.csdn.net/yongge/article/details/1930230
16. 相似度：0.33% 标题：《windows自带的ping和自己用ICMP实现ping有什...》
来源：https://bbs.csdn.net/topics/391990750?page=1
17. 相似度：0.31% 标题：《管理业务流程集成项目的基本原则》
来
源：https://www.ibm.com/developerworks/cn/rational/rationaledge/content/sep05/higgins/index.htm
18. 相似度：0.30% 标题：《电影院信息管理系统设计(可编辑)doc下载》
来源：https://ishare.iask.sina.com.cn/f/bwlhG4LXDyJ.html
19. 相似度：0.30% 标题：《数字图像处理技术现状展望论文资源》
来源：https://download.csdn.net/search/16002/10/0/0/1/板惧澶扮跺璁烘
20. 相似度：0.30% 标题：《当当云阅读》
来源：http://e.dangdang.com/h5/xinzhili_1.html
21. 相似度：0.29% 标题：《渗透测试中信息收集的那些事》
来源：https://blog.csdn.net/weixin_30732825/article/details/95112913
22. 相似度：0.28% 标题：《软件项目解决方案模板》
来源：https://blog.csdn.net/weixin_30586257/article/details/97015884
23. 相似度：0.26% 标题：《继承多态or与文件资源》
来
源：https://download.csdn.net/search/0/4/0/0/1/%E7%BB%A7%E6%89%BF%E5%A4%9A%E6%80%81
24. 相似度：0.26% 标题：《进程、线程、同步、通信、调度、死锁、存储管理.....》
来源：https://blog.csdn.net/yy2017220302028/article/details/104898711
25. 相似度：0.26% 标题：《技术面知识点总结》
来源：https://blog.csdn.net/qq_15437629/article/details/52388685
26. 相似度：0.26% 标题：《判断一个程序启动完成资源》
来
源：https://download.csdn.net/search/0/1/0/0/1/%E5%88%A4%E6%96%AD%E4%B8%80%E4%B8%AA
27. 相似度：0.26% 标题：《判断一个程序启动完成资源》
来
源：https://download.csdn.net/search/0/10/0/0/1/%E5%88%A4%E6%96%AD%E4%B8%80%E4%B8%A
28. 相似度：0.26% 标题：《继承多态or与文件资源》
来
源：https://download.csdn.net/search/0/1/0/0/1/%E7%BB%A7%E6%89%BF%E5%A4%9A%E6%80%81
29. 相似度：0.26% 标题：《TCP/IP第三层》
来源：https://blog.csdn.net/hguisu/article/details/8583552
30. 相似度：0.26% 标题：《Qt(7)Qt界面布局管理详解 – 滴滴咚咚》
来源：https://www.dididongdong.com/archives/6445
31. 相似度：0.26% 标题：《【pyqt5和wxpython】》
来源：https://www.csdn.net/gather_2d/Mtjakg3sNDQ4LWJsb2cO0O0O.html
32. 相似度：0.25% 标题：《网络扫描┅非常不错的文章，主要分为端口扫描（确定开放服务）...》
来源：https://www.cnblogs.com/bonelee/p/12687056.html
33. 相似度：0.25% 标题：《模块设计方法》
来源：https://blog.csdn.net/guotufu/article/details/83532826
34. 相似度：0.25% 标题：《转 黑客入门完整版教程》
来源：https://blog.csdn.net/Reincarn/article/details/90769721
35. 相似度：0.25% 标题：《一文搞懂交换基础知识》
来源：http://m.solves.com.cn/it/wl/yj/2020-03-02/12554.html

36. 相似度：0.22% 标题：《论文致谢模板》
来源：http://www.qt8.cc/list/lunwenzhixiemoban/
37. 相似度：0.22% 标题：《第 1 章 遗失的代码库》
来源：https://www.ituring.com.cn/book/tupubarticle/25580
38. 相似度：0.22% 标题：《计算机网络技术》
来源：https://blog.csdn.net/Assassin660/article/details/104948016
39. 相似度：0.20% 标题：《毕业论文致谢结束语.doc》
来源：https://max.book118.com/html/2017/0611/113448969.shtm
40. 相似度：0.19% 标题：《两个不同网段的IP地址能ping通，但是为什么不能在ARP上...》
来源：https://www.zhihu.com/question/20579906
41. 相似度：0.17% 标题：《高清在线不卡一区二区》
来源：http://www.wdrnezo.cn/14e1/brqpe
42. 相似度：0.16% 标题：《tech》
来源：https://www.zhihu.com/collection/189601219
43. 相似度：0.15% 标题：《Unity3D游戏框架设计》
来源：https://blog.csdn.net/aawoe/article/details/80903614
44. 相似度：0.14% 标题：《Python浅析线程（threading模块）和进程（pro...》
来源：https://www.cnblogs.com/tu240302975/p/12512826.html
45. 相似度：0.12% 标题：《怎样写论文的绪论，能为我提供一篇范文吗？》
来源：https://zhidao.baidu.com/question/205136643.html
46. 相似度：0.12% 标题：《怎么写好论文引言？》
来源：https://www.zhihu.com/question/57366545
47. 相似度：0.12% 标题：《TCP/IP协议学习导览》
来源：https://my.oschina.net/lscherish/blog/3197027/print
48. 相似度：0.12% 标题：《论文培养孩子细心和耐心摘要怎么写》
来源：https://zhidao.baidu.com/question/1831763198118574180.html
49. 相似度：0.12% 标题：《毕业论文前言引言怎么写》
来源：https://wenda.so.com/q/1462597489726414
50. 相似度：0.07% 标题：《关于电子商务实训平台的构建及在教学中实际运用的研究word免...》
来源：https://ishare.iask.sina.com.cn/f/30ZgzeeFG6k.html
51. 相似度：0.07% 标题：《单词句型汇总》
来源：https://blog.csdn.net/sinat_18722475/article/details/63685146
52. 相似度：0.07% 标题：《毕业设计选题系统设计与实现本科毕业设计论文(可编辑)doc下...》
来源：https://ishare.iask.sina.com.cn/f/19r34Gfzis3.html
53. 相似度：0.06% 标题：《图书借阅与推荐系统的设计与实现word免费下载》
来源：https://ishare.iask.sina.com.cn/f/19d4NmqVkk5.html
54. 相似度：0.06% 标题：《Linux多线程（五）多线程访问共享资源》
来源：https://blog.csdn.net/qq_38211852/article/details/80362696
55. 相似度：0.06% 标题：《基于J2EE和工作流技术的质量管理系统设计与开发》
来源：https://ishare.iask.sina.com.cn/f/btAUUtS9aaz.html

全文简明报告

编号：
桂林电子科技大学信息科技学院
毕业设计(论文)说明书
题 目： 网络扫描器
的设计与实现
系 别： 信息工程系
专 业： 计算机科学与技术 1
学生姓名： 陈彦志 1
学 号： 1651200111
指导教师单位： 计算机与信息安全学院
姓 名： 姚罡
职 称： 讲师
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 应用研究

2020年 5月 29日
独 创 性 声 明
本人郑重声明：所呈交的学位论文，是本人在导师的指导下，独立进行研究工作所取得的成果。除文中已经注明引用的内容外，本论文不含任何其他个人或集体已经发表或撰写过的作品成果。对本文的研究做出重要贡献的个人和集体，均已在文中以明确方式标明。本人完全意识到本声明的法律结果由本人承担。
学位论文作者签名： 日期：2020年5月29日
关于学位论文版权使用授权的说明

{100% 本人完全了解桂林电子科技大学信息科技学院关于收集、保存、使用学位论文的以下规定：学院有权采用影印、缩印、扫描、数字化或其它手段保存论文；}{100% 学院有权提供本学位论文全文或者部分内容的阅览服务；}{100% 学院有权将学位论文的全部或部分内容编入有关数据库进行检索、交流；}{100% 学院有权向国家有关部门或者机构送交论文的复印件和电子版。}

学位论文作者签名： 日期：2020年5月29日
导师签名： 日期：2020年5月29日
摘 要

{67% 信息收集是指为了更加有效地实施渗透测试而在测试前或测试过程中对目标的所有探测活动。}{52% 信息收集对于渗透测试整个流程的重要性是不言而喻的，可以说信息收集的完整性就决定了你的渗透测试结果。}{62% “知己知彼，百战不殆”，同时，信息收集对于了解组织安全架构、缩小攻击范围、描绘网络拓扑、建立脆弱点数据库等等都有很大的作用，}因此，设计一款方便易操作的网络扫描器对于网络管理员或者其他渗透测试人员来说是非常必不可少的。

我对目前已有的一些网络扫描器，比如Nmap、Zenmap做了一些比较详细的对比，发现这些扫描器都或多或少存在着一些不足之处，比如：nmap是控制台黑窗口程序，对于普通用户并不是很友好，在使用前需要对其的一些参数有所了解，并且如果事先不知道输入格式而盲目输入的话结果可能会事与愿违，另外，Zenmap虽然是图形化界面版本，但显示的却是英文，对于英文不是太好的测试人员来说使用起来会有些难度，此外，Zenmap的可选配置并没有体现出它的每个可选配置选项具体是使用了哪种扫描方法，对于想要对比各个方式间扫描效果差异的学习者来说，Zenmap可能并不是一个很好的选择，最后，这些扫描器大多只能提供主机探测、端口扫描、操作系统以及服务的识别而不能进行ftp弱口令和SQL注入漏洞的检测。所以，针对以上问题，我提出了我的网络扫描器的系统设计方案。

在我的方案中，我采用了按功能划分的模块化设计方法，降低了耦合，提高了系统的鲁棒性。系统共分为了三个主模块，分别是信息收集、漏洞扫描、图形化界面封装。信息收集模块能够进行主机探测、端口扫描、服务和操作系统识别；漏洞扫描模块实现了用户使用数据库时对SQL注入漏洞的检测以及文件传输过程中对FTP弱口令的检测；图形化界面封装模块实现了系统的图形化。

{63% 在扫描系统的具体实现中，我主要利用了scapy模块通过自己构造相应的包实现了icmp扫描、arp扫描、syn扫描、fin扫描、null扫描、xmas扫描和udp扫描的方法，}然后通过调用nmap实现了服务识别，操作系统探测是我通过搜集相关文献找到的一些方法实现的，ftp弱口令检测使用了匿名登录和词典爆破两种方法。SQL注入检测这块由于本人能力有限，所以只用到了一些非常简单的检测手段。此外，为了提高扫描效率，我使用了多线程的技术，最后通过QT5对软件进行了GUI的封装，完成了图形化界面的效果。

关键字：主机探测、端口探测、FTP检测、SQL注入检测、QT5、python、多线程
Abstract

Information collection refers to all detection activities of targets before or during testing in order to implement penetration testing more effectively.{62% The importance of information collection for the entire process of penetration testing is self-evident.} It can be said that the completeness of information collection determines your penetration test results.{53% "Know yourselves and know each other, you can fight forever", at the same time, information collection has a great role in understanding the organization's security architecture, narrowing the scope of the attack, depicting the network topology, establishing a vulnerability database, etc.} It is very essential for network administrators or other penetration testers.

I made some more detailed comparisons of some existing network scanners, such as Nmap and Zenmap, and found that these scanners have some more or less shortcomings. For example: nmap is a console black window program. Ordinary users are not very friendly, they need to understand some of their parameters before use, and if they do not know the input format in advance and enter them blindly, the result may be counterproductive. In addition, although Zenmap is a graphical interface version, it displays It is English. It is difficult for testers who are not too good in

English. In addition, the optional configuration of Zenmap does not reflect the specific scanning method used for each of its optional configuration options. Comparing learners who have different scanning effects between different methods, Zenmap may not be a good choice. Finally, most of these scanners can only provide host detection, port scanning, operating system and service identification instead of weak FTP passwords. And SQL injection vulnerability detection. Therefore, in response to the above problems, I put forward a system design solution for my network scanner.

{57% In my scheme, I adopted a modular design method divided by function, which reduces the coupling and improves the robustness of the system.} The system is divided into three main modules, namely information collection, vulnerability scanning, and graphical interface packaging. The information collection module can perform host detection, port scanning, service and operating system identification;{59% the vulnerability scanning module implements the detection of SQL injection vulnerabilities when users use the database and the detection of FTP weak passwords during file transfer;}{59% the implementation of the graphical interface packaging module The system is graphical.}

In the specific implementation of the scanning system, I mainly used the scapy module to implement the icmp scan, arp scan, syn scan, fin scan, null scan, xmas scan, and udp scan by constructing the corresponding package by myself, and then implemented by calling nmap For service identification, operating system detection is achieved by some methods I found by collecting relevant literature. FTP weak password detection uses anonymous login and dictionary blasting. Due to my limited ability of SQL injection detection, only some very simple detection methods are used.{54% In addition, in order to improve the scanning efficiency, I used multi-thread technology, and finally packaged the GUI through QT5 to complete the effect of the graphical interface.}

Keywords: host detection, port detection, FTP detection, SQL injection detection, QT5, python, multithreading

目 录

引言

{87% 如果把网络信息安全工作比作一场战争的话，网络扫描器就是这场战争中盘旋在终端设备和网络设备上空的“全球鹰”。}{100% 网络安全工作是防守和进攻的博弈，是保证信息安全、工作顺利开展的奠基石。}{91% 及时和准确地审视自己信息化工作的弱点、审视自己信息平台的漏洞和问题，才能在这场信息安全战争中，处于先机、立于不败之地。}{100% 只有做到自身的安全，才能立足本职，保证公司业务稳健的运行，这是信息时代开展工作的第一步。}{71% 网络扫描器，就是保证这场信息战争胜利的开始，它及时准确的察觉到信息平台基础架构的安全，}{100% 保证业务顺利的开展，保证业务高效迅速的发展，维护公司，企业，国家所有信息资产的安全。}

1 绪论

1.1 研究背景及意义

{57% 网络的不断发展不仅带给了人们极大的便利，同时也带来了一个巨大的潜在问题，网络安全。}{78% 近年来，网络中的安全事故频频出现，2019年7月，美国银行第一资本金融公司披露，一名黑客获取了逾1亿名顾客和潜在顾客的个人信息，包括姓名、地址、电话号码和生日。}{100% 2019年10月28日，格鲁吉亚遭到了大规模网络袭击，包括政府机构、新闻媒体在内的超过15000个网站被破坏，其中包括总统的个人网站主页。}{83% 2019年12月13日，美国南部路易斯安那州新奥尔良市遭到网络攻击，市长拉托亚坎特雷尔当日宣布该市进入紧急状态……这些网络安全事故严重影响了互联网的健康发展。}{58% 而造成这些问题的根本原因就是恶意攻击者发现了目标计算机可以利用的某些漏洞，然后利用这列漏洞在未授权的情况下访问甚至破坏目标系统，从而达到其非法目的。}对目标公司乃至个人造成了巨大的损失。所以，要想维护计算机系统的正常运行，防止不法分子对其进行破坏利用，就必须在恶意攻击者攻击之前，{52% 发现并解决存在于计算机系统中的这些漏洞，防患于未然。}

网络扫描器就是这样一类工具，它的原理就是模拟恶意工作者的工作方式，判断目标系统是否存在某些可被利用的漏洞来提前对其修补，因此网络扫描技术越来越受到人们的重视，研究网络扫描技术是很有意义的。

1.2 主要研究的内容

本文的主要工作是设计与实现一个网络扫描器，具体工作内容如下：

{58% 1）通过对现有网络扫描工具的分析和比较，对这些软件的功能和工作步骤进行详细了解。}掌握要实现网络扫描工具所必须要知道的理论基础，包括网络协议、多线程、PyQt5以及编程实现的基础知识等等，同时对网络扫描技术的实现原理、特点进行分析，并对各个技术的不同和优缺点进行分析比较，比如多线程和多进程之间进行对比等等。

2）在了解了基础理论后，开始着手设计实现网络扫描器。{58% 系统将按功能划分的模块化思路来设计网络扫描器的总体结构和各个功能模块，并对各个模块的设计方法及其实现给出比较详细的陈述。}该网络扫描器将包含信息搜集模块、漏洞检测模块和GUI图形封装模块。其中信息搜集主模块包含主机存活探测子模块、端口扫描子模块、端口服务识别子模块和操作系统识别子模块，漏洞扫描主模块包含SQL注入漏洞检测子模块和文件传输过程对FTP弱口令检测子模块。

1.3 论文的结构安排

1）绪论。{65% 首先简单介绍了课题的研究背景意义及其相关技术的国内外研究现状，其次简要的说明课题的主要研究内容和论文的结构安排，最后给出了本系统的开发环境。}

{55% 2）网络扫描技术的分析。}主要是对我使用的网络扫描技术做的一个简单介绍，包括主机探测、端口探测、操作系统指纹识别技术和FTP弱口令检测还有SQL注入漏洞检测的原理，最后通过对多线程和多进程的对比来说明我为什么使用多线程以及为什么使用QT5来进行可视化界面的设计。

3）网络扫描器的设计。{64% 首先，给出系统的需求分析，包含需求分析概述、功能需求概述、用户对系统的需求概述，然后是总体设计，包括设计思路、设计目标以及系统总体框架;}{73% 最后，对系统的各个功能模块的设计进行详细的介绍。}

4）网络扫描器的实现。{61% 首先对于系统需要用到的基本工具框架进行阐述，包括scapy的使用、shodan的使用、ip地址的解析和PyQt5的使用，之后给出各个模块的具体方法的具体实现。}

{60% 5）系统测试与分析。}{60% 首先介绍了测试环境与测试对象，最后使用本文所设计的网络扫描器对目标主机进行测试。}

{80% 6）全文总结与展望。}{54% 首先，对论文的工作进行简单的概述，概述中主要包含自己的创新内容;}其次，给出本次系统设计中存在的一些问题，希望能在以后的工作中得到解决。

1.4 系统的开发环境

1）操作系统：macOS Catalina 10.15.3
2）编程语言：python 3.7.4
3）集成开发环境：pycharm professional 2019.2
4）数据包处理工具：scapy 2.4.3
5）获取测试样例：shodan
6）GUI程序开发框架：PyQt5 5.14.1

2 网络扫描技术的分析

2.1 主机探测

主机探测主要使用了四种方法，分别是：ARP探测，ICMP探测，TCP SYN 443端口探测，TCP ACK 80端口探测，他们全部使用scapy来实现发包收包。

1）ARP探测原理：

{69% ① 本地主机在局域网中广播arp请求，arp请求数据帧中包含目的主机的ip地址。}{76% 翻译一下就是，如果你是这个ip的拥有者，请回答你的硬件地址。}

{63% ② 目的主机的arp层解析这份广播报文，识别出是询问其硬件地址。}{57% 于是发送arp应答包，里面包含ip地址及其对应的硬件地址。}翻译一下是，你问的ip地址的所有者就是我，我的mac是xx:xx:xx...

③ 本地主机收到arp应答后即可判定目的主机在线。

2）ICMP探测原理：

其实，两台网络设备互ping，是有两种的。

1.同一网段

{73% ① 如图，主机A ping 主机B，那么主机A要先封装二层报文，它会先查自己的MAC地址表，如果没有B的MAC地址，就会向外发送一个ARP广播包。}

{80% ② 交换机收到这个报文后，交换机有学习MAC地址的功能，所以它会检索自己有没有保存主机B的MAC地址。}

③ 如果有，就返回给主机A，如果没有，就会向所有端口发送ARP广播，其他主机收到后发现不是在找自己

就纷纷丢弃该报文，不去理会。

{66% ④ 直到主机B收到报文后就立即响应，B的MAC地址是多少，同时学到主机A的MAC地址，并按同样的ARP报文格式返回给主机A，如图。}

{60% ⑤ 这时候主机A学习了主机B的MAC地址，然后就把这个MAC封装到ICMP协议的二层报文中向主机B发送。}

{58% ⑥ 主机B收到这个报文后，发现是主机A的ICMP回显请求，就会按照同样的格式，返回一个值给主机A，主机收到这个值即可判定主机B在线。}

2.不同网段

{60% ① 主机A ping 主机C，主机A发现主机C的IP和自己不是同一网段，主机A就会去找网关转发。}

{74% ② 它会像同一网段中的步骤①一样先发送一个ARP广播，学到网关的MAC地址，再发封装ICMP报文给网关路由器。}

{62% ③ 路由器收到主机A发过来的ICMP报文，发现目的MAC是其本身，根据目的IP查路由表，然后去掉原来的MAC头部，加上自己的MAC地址向主机C转发。}

④ 如果网关也没有主机C的MAC地址，同样需要ARP广播一下即可相互学到。

{53% ⑤ 路由器2端口能学到主机C的MAC地址，主机C也能学到路由器2端口的MAC地址。}

⑥ 最后，主机C已学到路由器2端口的MAC，路由器2端口转发给路由器1端口。

{57% ⑦ 路由器1端口学到主机A的MAC地址的情况下就将ICMP的回显请求回复过来，主机A收到回复，判定主机C在线。}

3）TCP SYN 443端口探测原理：

{59% TCP SYN扫描又称半开式扫描，该过程不会和服务端建立完整的连接， }

① 首先本地主机会发送一个带有SYN标识和443端口号的TCP数据包给目的主机。

② 如果目的主机的这个端口是开放的，则会接受这个连接并返回一个带有SYN和ACK标识的数据包给本地主机，如果443端口处于关闭状态，则目的主机会返回一个RST标识的数据包。

③ 只要本地主机收到目的主机发来的数据包（不管是SYN和ACK还是RST），即可判定目的主机在线。

4）TCP ACK 80 端口探测原理：

① 本地主机发送一个带有ACK标识和80端口号的TCP报文给目的主机。

② 目的主机无论端口是否开放都会返回一个flags为RST的包，但如果目的主机没有在线的话就会一个数据包都不返回，

2.2 端口探测

端口探测使用了五种方法，分别是TCP SYN 端口扫描、TCP FIN 端口扫描、TCP NULL 端口扫描、TCP XMAS端口扫描、UDP端口扫描，其中TCP NULL 端口扫描和TCP XMAS端口扫描类似，它们共同的特点是能够躲避防火墙、包过滤器和日志审计，逃避入侵检测系统 IDS 等。

1）TCP SYN 端口扫描原理：

{53% 如主机探测中TCP SYN 443端口探测中所述，TCP SYN扫描又称半开式扫描，该过程不会和目的主机建立完整的连接。}

① 本地主机发送一个带有SYN标识和端口号的TCP数据包给目的主机。

② 如果目的主机的这个端口是开放的，则会接受这个连接并返回一个带有SYN和ACK标识的数据包给本地主机。

{59% ③ 本地主机收到这个带有SYN和ACK标识的数据包即可判定目的主机的这个端口是开放的。}

2）TCP FIN 端口扫描原理：

{62% 在发送的数据包中只设置FIN标志位，如果目标端口是开放的则不会回复任何信息。}{59% 如果目标端口关闭则会返回一个RST+ACK的数据包。}

3）TCP NULL 端口扫描原理：

{61% 在发送的数据包中不设置任何标志位(tcp标志头是0)，如果目标端口是开放的则不会回复任何信息。}

{59% 如果目标端口关闭则会返回一个RST+ACK的数据包， }

4）TCP XMAS端口扫描原理：

{61% 在发送的数据包中设置PSH,FIN,URG标志位，如果目标端口是开放的则不会回复任何信息。}{59% 如果目标端口关闭则会返回一个RST+ACK的数据包。}

5）UDP 端口扫描原理：

因为它是无连接不可靠的协议，发送数据包过去以后，通常也不会有任何的对等回应。因此，本系统使用UDP扫描无法确定某个端口是否一定开放，只能说，如果发送UDP数据包过去之后没有收到相应数据包，那么就说明这个端口可能是开放的。

2.3 操作系统指纹识别技术

通过查阅相关文献找到了六种识别操作系统的方法，分别是：

1）根据ICMP数据包的TTL值，向目标主机发送ICMP报文，大于64一般为Windows系列，小于等于64一般为Linux系列。

{63% 2）FIN探测，发送FIN包到打开端口，等待回应，RFC793定义的标准行为是不响应，但Windows会回应一个RESET包。}

{79% 3）标记位探测，在SYN包TCP头中设置未定义的TCP标记64或128，低于2.0.35版本的Linux会在回应包中保持此标记，其他OS几乎没有这个问题。}

{80% 4）TCP初始窗口，检查返回数据包的窗口大小，某些系统使用比较特殊的窗口值（Microsoft使用的窗口值总是0x402E）。}

5）ACK值，向一个关闭的TCP端口发送一个FIN
PSH

{68% URG包，许多OS会将ACK值设置为ISN值，但Windows会设置为 seq+1。}

{91% 6）服务类型TOS, 对于ICMP的“端口不可达”信息，经过对返回包的TOS值得检查，几乎所有OS使用ICMP错误类型0，而Linux使用的值是0xC0。}

2.4 FTP弱口令检测

有两种方法，分别是扫描匿名FTP和扫描FTP弱口令，可以通过Python的ftplib库中的Ftp这个类实现。

{53% 1）扫描匿名FTP：其实就是没有用户名和密码直接对目标主机进行FTP连接，FTP匿名登录的扫描主要应用于批量扫描中，}单独针对一个FTP服务器进行扫描的话成功几率比较小，不过也不排除成功的可能。

2）扫描FTP弱口令：其实就是暴力破解，但为何我们不称为暴力破解呢？因为我们只是扫描一些简单的密码组合，并不是所有可能的密码组合，而且我们也没有那么多时间去暴力破解。只是一个密码而已，弱口令扫不到就算了，直接去检测下一个目标主机。

2.5 SQL注入漏洞检测

主要使用单引号判断法和判断语句判断法。

1）单引号判断法：在参数后加单引号

{64% 如果页面返回错误，则存在 Sql 注入。} 因为无论字符型还是整型都会因为单引号个数不匹配而报错。如果未报错，不代表不存在 Sql 注入，因为有可能页面对单引号做了过滤，这时可以使用判断语句进行注入。

2）判断语句判断法：数据库表字段的数据类型有多种，但是所有这些数据类型，都可划分为“数字型”与“字符型”两大类。

数字型可以使用 and 1=1 和 and 1=2 来判断：

URL 地址中输入 http://xxx/abc.php?id= x and 1=1 页面依旧运行正常，继续进行下一步

URL 地址中继续输入 http://xxx/abc.php?id= x and 1=2 页面运行错误，则说明此 Sql 注入为数字型注入。

字符型可以使用 and '1'='1 和 and '1'='2来判断：

URL 地址中输入 http://xxx/abc.php?id= x' and '1'='1 页面运行正常，继续进行下一步。

URL 地址中继续输入 http://xxx/abc.php?id= x' and '1'='2 页面运行错误，则说明此 Sql 注入为字符型注

入。

2.6 Python中多线程和多进程的对比

线程是一个基本的 CPU 执行单元。它必须依托于进程存活。一个线程是一个execution context（执行上下文），即一个 CPU 执行时所需要的一串指令。

{95% 进程是指一个程序在给定数据集合上的一次执行过程，是系统进行资源分配和运行调用的独立单位。}{100% 可以简单地理解为操作系统中正在执行的程序。}{100% 也就说，每个应用程序都有一个自己的进程。}{100% 每一个进程启动时都会最先产生一个线程，即主线程。}{100% 然后主线程会再创建其他的子线程。}

Python多线程：CPU 是多核时是支持多个线程同时执行的。但在 Python 中，无论是单核还是多核，同时只能由一个线程在执行。其根源是因为GIL。{86% GIL 的全称是 Global Interpreter Lock(全局解释器锁)，这是为了数据安全所做的决定。}{83% 某个线程想要执行，必须先拿到 GIL，并且在一个 Python 进程中，GIL 只有一个。}{89% 拿不到GIL的线程，就不允许进入 CPU 执行。}{97% 每次释放 GIL锁，线程进行锁竞争、切换线程会消耗资源。}这就是为什么在多核CPU上，Python 的多线程效率并不高的根本原因。

{57% Python多进程：进程之间不共享数据。}如果进程之间需要进行通信，则要用到Queue模块。

通过实验测试发现，本系统因为使用scapy进行收包和发包，又因为scapy收包发包本身就慢，使用多线程和多进程效率都差不多，另外使用多进程如果速度过快的话，也因为网络延时的问题，会造成很多本该能收到的包收不到和报错“'L2bpfSocket' object has no attribute 'ins'”，另外本系统需要频繁进行输入输出操作，属于I/O 密集型，所以最终决定本系统使用多线程。

2.7 为什么使用PyQt5来进行可视化界面的设计

Python自带的Tkinter包设计GUI程序的功能比较弱，无论是美观上还是性能上都不是太令人满意。

{61% Qt C++类库是一套广泛使用的跨平台GUI设计类库，PyQt5是Qt5 C++类库的Python绑定，使用PyQt5在Python里编程，可以开发出比较专业的Python GUI应用程序，}不管在美观上还是在性能上都可以做到很理想，此外，PyQt5支持跨平台、文档比其他GUI库相对来说更加丰富同时又有方便的周边工具支持：QtDesigner。

所以，我决定使用PyQt5来进行本系统的可视化界面的设计。

3 网络扫描器的设计

3.1 系统需求分析

{55% 需求分析是一个项目设计与实现的开始更是整个过程中最关键的一个部分，如果在需求分析的时候就正确意识到了用户的需要的话，最后的作品或许更能令人满意。}否则的话，不能令人满意不说，浪费的人力物力更是巨大的。

3.1.1 功能需求概述

{55% 根据网络扫描器的业务需求，提供的具体功能如下：}

{57% 1）主机探测：探测目标主机是否在线，提供的主机探测方法有ARP扫描、ICMP扫描、SYN 443 端口扫描、TCP ACK 80 扫描。}

{70% 2）端口扫描：探测目标主机端口是否开放，提供的端口扫描方法有SYN扫描、FIN扫描、NULL扫描、XMAS扫描、UDP扫描。}

{57% 3）服务识别：探测目标主机开放端口上运行的具体软件。}

{54% 4）操作系统探测：探测目标主机操作系统。}

5）FTP弱口令检测：探测开放FTP服务的目标主机是否存在弱口令或者可以直接匿名登录。

6）SQL注入漏洞检测：探测目标主机是否含有SQL注入漏洞。

3.1.2 性能需求概述

1）主机探测：每秒探测30个以上ip地址。

2）端口扫描：每秒扫描30个以上端口。

3）服务识别：从开始执行到结束识别总共时间不能超过2分钟。

4）操作系统识别：从开始执行到结束识别总共时间不能超过2分钟。

5）FTP弱口令检测：每秒处理30个以上目标主机。

6）SQL注入漏洞检测：从开始执行到结束识别总共时间不能超过2分钟。

3.1.3 出错处理需求概述

1）主机探测：接收到一个错误输入会无法执行，开始探测按钮无法被按下，即使可以绕过系统也不会崩溃，而是返回“什么也没有探测到”消息。

2）端口扫描：接收到一个错误输入会无法执行，开始扫描按钮无法被按下，即使可以绕过系统也不会崩溃，而是返回“什么也没有扫描到”消息。

3）服务识别：接收到一个错误输入会无法执行，开始扫描按钮无法被按下，即使可以绕过系统也不会崩溃，而是返回“什么也没有探测到”消息。

4）操作系统识别：接收到一个错误输入会无法执行，开始扫描按钮无法被按下，即使可以绕过系统也不会崩溃，而是返回“什么也没有探测到”消息。

5）FTP弱口令检测：遇到错误的输入目标主机ip会直接跳过进行下一个目标主机的检测.

6）SQL注入漏洞检测：遇到错误的输入会直接返回“没有检测到SQL注入漏洞”消息。

3.1.4 用户对于系统需求概述

{56% 对于一个网络扫描器系统来说，在提供必要的功能的同时，也更应该方便用户的使用。}具体需求如下：

1）文件拖拽功能：在FTP弱口令检测界面的主机、用户名、密码文本框中既可以通过手动的方式输入，也可以直接将单个数据一行，每行以回车键分割的文本文件直接拖入文本框中以实现快速的输入。

2）探测方法清晰区分：在保证系统实用型的同时，将各个主机探测、端口扫描的方法清晰区分出来，这样可以有助于学习者来比较各个探测方法在效率方面和准确性方面的差异与优劣。

3）ip地址指定范围探测：本系统可以通过192.168.0.0/24、192.168.0.122、192.168.0.100-200三种格式来实现针对不同ip范围的扫描，帮助用户避免不必要的时间浪费在本不打算探测的ip地址上。

4）扫描探测的实时进度显示：在一个相对较长时间的扫描探测过程中，底部状态栏实时显示可以让用户追踪任务执行的进度，避免用户以为系统已经卡死，造成用户本可以不会有的对本系统的失去信心。

5）界面美观、输出易分辨

3.2 系统总体设计

{56% 设计系统时，系统的总体设计可以为系统后面的功能设计提供一个大的方向，此文主要从设计思路、设计目标和总体框架三方面进行讲述。}

3.2.1 设计思路

本系统的体系结构如下图所示：

{53% 整个系统的工作过程是：本地主机（用户）通过本系统扫描网络中的目标主机，然后将得到的结果返回给本地主机（用户）。}

{54% 本系统主要用于对目标主机基本信息的侦查和FTP弱口令以及SQL注入漏洞的检测，结合之前针对网络扫描技术的分析，给出本系统的总体设计路线：}

1）实现系统所必须的最基本功能，也就是网络扫描技术分析中的全部内容。

2）每个功能使用模块化设计，这样在增加或者修改模块时只需要改动相应模块即可同时也可提高系统的可扩展性。

{54% 3）主机探测和端口探测全部是先实现一个目标主机或者一个目标主机的一个端口的探测，然后通过多线程实现探测多个以加快速度。}

4）尽可能的完成需求分析中所要求的内容。

3.2.2 设计目标

这里的实际目标主要是与系统使用者所关联的整体需求目标，主要包括以下几个方面：

1）面向对象：主要面向渗透测试的学习者、学生和网络管理员。

2）用户界面：使用可视化界面，操作简单方便易学，不像命令行那样需要记住很多参数。

3）使用方便性：用户只需要在操作界面上输入目标主机，点击开始按钮即可进行扫描。

{55% 4）扫描的准确性：通过尽量平衡扫描的超时时间和用户的等待时间来尽力使得用户不至于等的时间太

长的同时能获得尽可能准确的结果。}

5）扫描的隐蔽性：因为本系统将各个扫描方法全部独立开，有些扫描方法的确能够躲避对方防火墙的检测，{63% 以及不能够被目标主机反向查出扫描主机的信息，比如，TCP NULL扫描和TCP XMAS扫描等，用户可以自主选择。}

6）扫描的速度：由上边的第四点也已经说明，本系统为了尽可能保证扫描的准确性而故意稍微减慢了一些扫描的速度但也不至于让用户无法忍受，本系统使用多线程技术和一些其他措施可以保证用户不会遇到无限等待的情况。

3.2.3 总体框架

{73% 本系统的总体框架图，如图所示： }

本系统采用模块化设计，主要包含信息搜集模块、漏洞检测模块和GUI图形封装模块。其中信息搜集主模块包含主机存活探测子模块、端口扫描子模块、端口服务识别子模块和操作系统识别子模块，漏洞扫描主模块包含SQL注入漏洞检测子模块和文件传输过程对FTP弱口令检测子模块。

{52% 模块化设计使得系统的设计思路更有条理，同时，系统的可扩展性也得到了提高。}由于各个模块的详细设计方法在之前网络扫描技术的分析中已经给出，在此不予赘述。

3.3 端口扫描的工作流程

本系统中大多数功能模块都是独立的，相互之间没有任何关联，但端口扫描除外，在进行端口扫描前需要先进行主机探测，如果主机本身就没有在线，那么探测端口也就没有丝毫意义，所以这里需要另外给出端口扫描的工作流程，如图所示。

4 网络扫描器的实现

4.1 系统实现的基础

4.1.1 Scapy的使用

Scapy是基于Python语言的网络报文处理程序，它可以让用户发送、嗅探、解析、以及伪造网络报文，运用Scapy可以进行网路侦测、端口扫描、路由追踪、以及网络攻击。本系统完全使用Scapy进行收包和发包。

使用Scapy前需要先下载并确保已经安装了Python3,在命令行输入以下内容即可下载。

具体如何使用可参考官方文档，此处省略。

4.1.2 shodan的使用

{86% 首先，Shodan 是一个搜索引擎，但它与 Google 这种搜索网址的搜索引擎不同，Shodan 是用来搜索网络空间中在线设备的，本系统通过调用python中的shodan模块使用shodan API进行获取FTP目标主机。}

使用shodan前需要先下载并确保已经安装了python3，在命令行输入以下内容即可下载。

之后还需要在shodan官网注册一个账号获取API_key，下图以获取FTP目标主机为例进行说明。

4.1.3 IP地址的解析

因为在可视化界面中可以输入三种格式的ip地址，分别是192.168.0.0/24、192.168.0.122、192.168.0.100-200，所以在真正执行程序前需要先把这些格式全部解析成单个的ip地址放入到一个列表中，后续的操作只需要遍历这个列表即可。解析ip地址我使用了正则匹配和字符串操作两种方法。

1）ip地址网段表示法解析

我使用的是python的ipaddress模块，然后将解析后的ip地址添加到一个新的列表中返回这个列表。

2）ip地址连字符格式解析

连字符这种格式的解析我使用的是字符串的一些操作方法，首先解析出连字符两边的数字，然后遍历这个区间，{64% 用前边的最后一个小数点前的字符串加上这个区间中的那个数字的组合就是一个完整的符合要求的ip地址，}这种方式其实比较的简陋，如果连字符后包含非数字是会报错的，所以我加了一个异常处理，如果报错那么就直接返回False，可视化界面那里接受到ip列表后会允许程序运行，如果接收到False那么用户就无法点击开始执行按钮。经过一些边界条件的测试发现我这样处理确实是可行的。

3）单个ip地址的校验

单个ip地址的格式需要校验一下，这里我使用的是正则表达式，如果能通过正则校验，那么我就添加到列表中然后返回这个列表。

4.1.4 PyQt5的使用

PyQt是Python语言的GUI编程解决方案之一。可以用来代替Python内置的Tkinter。相比其他python的GUI编程解决方案，PyQt相比起来功能更强大，性能更好，所以本系统使用QtQt5进行可视化界面的设计。

使用PyQt5前需要先下载并确保已经安装了python3，在命令行输入以下内容即可下载。

本系统使用专门的一个类进行UI窗体的设计，通过单继承与界面独立封装方法实现界面与业务逻辑分离。通过下图的例子简单介绍这种单继承的方法。

{58% 在本例中，新定义的窗体业务逻辑类QmyWidget只有一个基类QWidget,在QmyWidget的构造函数中，首先调用父类（也就是QWidget）的构造函数，这样self就是一个QWidget对象。}然后显式地创建了一个UI_FormHello类的私有属性self.__ui。{59% 该私有属性包含可视化设计的UI窗体上的所有组件，只有通过self.__ui才可以访问窗体上的组件，包括调用其创建界面组件的setupUI()函数。}

通过使用如下方式，它可以有以下几个优点：

{58% 1）在QmyWidget类的内部对窗体上的组件的访问都通过这个属性实现，而外部无法直接访问窗体上的对象，这样更加符合面向对象封装隔离的设计思想。}

{54% 2）窗体上的组件不会与QmyWidget里定义的属性混淆，例如下面的语句：}

self.__ui.LabHello表示窗体上的标签对象LabHello，它是self.__ui的一个属性；self.Lab是QmyWidget类里定义的一个属性。{53% 这样，窗体上的对象和QmyWidget类里新定义的属性不会混淆，有利于界面与业务逻辑的分离。}

4.2 信息收集模块的实现

首先需要说明一下scapy中标志位（flags）的四种表达方式，下文需要用得到。

4.2.1 主机存活探测子模块的实现

主机存活探测共包含四种：arp探测、icmp探测、syn_443端口探测、ack_80端口探测。具体探测方法在上文网络扫描技术的分析中已经给出，全部都是先实现探测一个，然后再使用多线程技术实现对多个目标主机的探测，这里先以arp探测为例给出多线程的实现然后给出主机存活探测各种方法的具体实现。

{57% ip_list是经过解析后的目标主机列表，因为最开始我使用的是多进程技术，所以使用了进程队列实现进程之间的通信，}后来改成了多线程后因为这个进程队列对程序执行和执行结果都没有影响所以就保留了下来，经过执行多线程后，结果都保存在了队列中，然后将结果队列中的元素添加到一个新的列表中返回这个列表。其他探测方法的多线程实现与此类似，故省略。

1）arp探测：
2）icmp探测：
3）syn_443端口探测：
4）ack_80端口探测：

上述四种方法的具体实现格式大致相同，所以在此统一叙述，首先使用scapy构造相应的包，然后使用sr或者srp发包函数进行发送，如果能够收到响应包，那么就将相应的想要的数据放入进程队列中返回。

其中，sr和srp的区别是srp关注数据链路层，所以可以看到在arp探测时用到了srp发包函数。

4.2.2 端口扫描子模块的实现

{67% 端口扫描与主机探测的模式相似，再次不做过多赘述，直接给出syn扫描、fin扫描、udp扫描、null扫描、xmas扫描的具体实现。}

1）syn扫描：
2）fin扫描
3）udp扫描
4）null扫描
5）xmas扫描

4.2.3 端口服务识别子模块的实现

服务识别模块可以探测到开放端口正在运行的具体软件，我是通过直接调用nmap实现的，使用nmap前需要先下载，通过以下命令即可下载。

以下是服务识别的具体实现：

4.2.4 操作系统识别子模块的实现

本系统提供六种方法实现识别操作系统，因为识别操作系统不可能非常的准确，可能一种方法探测出目标主机是Linux而使用另一种方法探测出来却是Windows，如果只是将每种方法的探测结果简单罗列出来可能对于用户来说看起来不是很方便，所以我将最终结果以概率的形式展示出来，对于用户来说可能这样会更加清晰。

具体实现首先我是通过先增加两个变量和一个列表，分别是os_windows_rate代表是Windows系统的概率、os_linux_rate代表是linux的概率、os_is_linux是一个列表且只能存储0和1，其中的元素为每种方法探测出来的结果，列表中的0元素表示探测结果为Windows，列表中1元素表示探测结果为linux。六种探测方法全部执行完毕后取得os_is_linux中元素的数量num，os_is_linux中0元素的数量windows_num，os_is_linux中1元素的数量linux_num。

os_windows_rate = windows_num / num
os_linux_rate = linux_num / num
以下为各种探测方法的具体实现

1）根据ICMP数据包的TTL值，向目标主机发送ICMP报文，大于64一般为Windows系列，小于等于64一般为Linux系列。

{63% 2）FIN探测，发送FIN包到打开端口，等待回应，RFC793定义的标准行为是不响应，但Windows会回应一个RESET包。}

其中的port_list为使用syn端口扫描探测到的开放端口，具体syn端口扫描实现上文已有讲述，故省略。

{79% 3）标记位探测，在SYN包TCP头中设置未定义的TCP标记64或128，低于2.0.35版本的Linux会在回应包中保持此标记，其他OS几乎没有这个问题。}

{80% 4）TCP初始窗口，检查返回数据包的窗口大小，某些系统使用比较特殊的窗口值（Microsoft使用的窗口值总是0x402E）。}

5）ACK值，向一个关闭的TCP端口发送一个FIN
PSH

{68% URG包，许多OS会将ACK值设置为ISN值，但Windows会设置为 seq+1。}

{88% 6）服务类型TOS, 对于ICMP的“端口不可达”信息，经过对返回包的TOS值得检查，几乎所有OS使用ICMP错误类型0，而Linux使用的值是0xC0。}

4.3 漏洞扫描模块的实现
4.3.1 FTP弱口令检测子模块的实现

两种方法实现ftp弱口令探测，分别是匿名登录和暴力破解。

1）匿名登录，如果报错说明登录失败，直接用异常处理跳过即可，否则说明登陆成功。

2）扫描FTP弱口令：同上，报错直接用异常处理跳过。

此外，username和password是由相应字典文件拖拽入可视化界面的面板后经过解析后产生的字典列表中的元素。FTP弱口令检测用到了多线程，下图为FTP弱口令扫描的多线程实现。

4.3.2 SQL注入漏洞检测子模块的实现
5系统测试与分析
5.1 测试的作用与意义

{100% 软件测试是程序的一种执行过程，目的是尽可能发现并改正被测试软件中的错误，提高软件的可靠性。}{100% 它是软件生命周期中一项非常重要且非常复杂的工作，对软件可靠性保证具有极其重要的意义。}

5.2 测试环境
扫描主机的ip是：192.168.43.182， 操作系统是macOS Catalina 10.15.3
5.3 测试用例

本测试连接的是手机的热点，ip为192.168.43.41，与本地主机同时连接手机热点的有ipad，ip为192.168.43.236，同时，在本地主机又开了两个虚拟机，分别是metasploitable2和win10，metasploitable2的ip为192.168.43.46，win10的ip为192.168.43.52。

5.4 测试结果
5.4.1 主机探测测试结果
1）arp探测

2）icmp探测
3）syn_443端口探测
4）ack_80端口探测

通过上图四种主机探测方法可以发现主机探测子模块成功探测到了所有在线的目标主机，完美完成任务。

5.4.2 端口扫描测试结果
为了节省篇幅，这里仅以192.168.43.46，前100个端口为例。
1）syn扫描
2）fin扫描

对于fin端口扫描，Windows和linux返回的包并不相同，所以使用fin端口扫描无法准确的扫描出Windows主机的开放端口。

3）null扫描
4）xmas扫描
5）udp扫描

因为udp是无连接不可靠协议，所以用于端口扫描很不准确，只能做一个大概检测。

5.4.3 服务识别测试结果
5.4.4 操作系统识别测试结果
5.4.4 FTP弱口令检测测试结果
5.4.5 SQL注入漏洞检测测试结果
6 全文总结与展望
6.1 全文总结

本系统按功能模块主要分为信息收集模块、漏洞扫描模块和GUI图形化封装模块，因为GUI图形化封装模块主要是可视化界面的设计，对于系统功能逻辑方面设计较少，所以本文并没有做过多的叙述。

信息收集模块主要包含主机探测、端口扫描、服务识别和操作系统探测，主机探测包含arp探测、icmp探测、syn_443端口探测、ack_80端口探测，{62% 端口扫描主要包含syn扫描、fin扫描、udp扫描、null扫描、xmas扫描，其中主机探测和端口扫描的具体实现方法全部为先实现一个然后使用多线程技术实现探测多个，}同时收包发包由scapy实现，服务识别的功能是探测出开放端口上正在运行的具体软件，这项功能由调用nmap实现，然后是操作系统探测，方法是由我在网上搜集文献资料找到然后用scapy实现的。

漏洞扫描模块包含ftp弱口令检测和sql注入漏洞检测，ftp弱口令检测主要使用两种方法，分别是匿名登录和字典爆破，由ftplib实现，这部分的难点不在功能逻辑上，而是在于可视化界面文件拖拽那里。最后是sql注入漏洞检测，这部分做的比较简单，只使用了单引号和几个判断语句进行判断而已。

{55% 通过最终的软件测试结果得知，本系统的各个模块都很好地完成了任务，信息收集模块成功的对目标主机的信息进行了收集，}同时漏洞扫描模块也基本完成了任务，只是因为爆破字典一般所以在ftp字典爆破那里表现不佳。

6.2 后续工作与展望

在实现本系统的过程中，由于本人的水平有限再加上时间的原因，并没能把本系统做的尽善尽美，还存在着许多没能解决的问题等待着日后区解决，这些问题主要包括：

1）可视化界面没能做到完全的实时进度显示，虽然可视化界面底部的状态栏可以做到实时显示，但输出数据的文本控件必须等到所有数据全部处理完才能显示，不能做到探测到一个输出一个，如果想解决这个问题需要对线程的深入理解。

2）服务识别那里限于本人的水平，是调用nmap实现的，在执行服务识别时可视化界面会短暂的卡住，这里有两个需要改善的点，一是替换掉nmap，自己实现这个功能，二是解决执行服务识别会卡住这个问题。

3）操作系统识别那里只用到了六个方法，而且有几个方法已经很老了，对于判断操作系统其实还远远不够，还需要完善识别操作系统的方法。

4）SQL注入检测做得实在是太简单了，这块儿也很需要在未来工作中进一步去完善。

致 谢

大学四年这么快就过去了，回首这四年，收获了太多的成长，同时也认识到了自己很多的缺点。四年时间里，看了很多优质的书，对我三观的构造有着决定性的作用，像《态度》、《激荡三十年》、《如何阅读一本书》、《人类简史》、《把时间当做朋友》、《穷查理宝典》等等，从格局到做事方法和思考角度等都让

我深受启发。感谢他们，

感谢姚罡老师，毕业论文给了我很多的指导，尤其是有次老师给我打电话说回校了如果需要自己可以进山当面帮我解决，真的让我非常非常感动。此外，在做毕业设计期间，很多问了之后觉得很幼稚的问题老师还是很耐心的给我解答，我感觉我可能是我们几个选了姚罡老师毕业论文的人里边最烦的了。这个毕业论文是我大学期间可以说是用时最长、用心最多的了，参考了很多文献资料，本打算三月底就要完成的硬生生向后拖了一个月，其实还是自己的代码功底太弱，做的时候感觉好难但等做完了再回过头看我的代码，感觉很简单嘛，很多python里边高级的东西，比如GIL、垃圾回收、性能陷阱、锁等等都没有涉及到，本还打算在实现sql注入期间将sqlmap的源码好好读一读，但对于我来说实在是太费劲了，当然我也没有说我放弃，等我有时间我一定会再回过头来重新读sqlmap源码的。

{62% 最后，还要感谢我的家人，大学四年一直都在默默的支持着我，支持着我做的决定，给我鼓励，家里虽然那么忙，}却给我提供了一个那么好、那么安静的环境不打扰我学习，一直尽力给我提供最好的物质条件，没有给我任何其他方面的压力，不至于让我分心，让我安安心心的平稳度过了四年，谢谢他们。

参考文献

[1] 刘英,薛质,王轶骏.基于TCP协议可选项的远程操作系统识别[J].信息安全与通信保 密,2007,11:71-72.
[2] 陈昊.综合扫描系统的设计与实现[D].成都:电子科技大学,2017.
[3] 李瑞民.网络端口扫描技术的研究与实现[D].郑州:中国人民解放军信息工程大学,2002.
[4] 沙 超, 陈云芳.一种基于 TCP/IP 协议栈的操作系统识别技术[J].计 算 机 技 术 与 发 展,2006,16(10):125-127.
[5] 林天峰.操作系统类型识别方法[J].计 算 机 与 现 代 化,2003,11:21-23.
[6] 蔡岚岚.浅谈操作系统指纹识别[J].科技信息,2011,36:258.
[7] 张焕明,宋振锋.识别操作系统的方法、原理及其防范技术[J].中山大学学报 (自然科学 版),2002,41(S1):49-52.
[8] Smita Patil，Nilesh Marathe，Puja Padiya. Design of efficient web vulnerability scanner[C].International Conference on Inventive Computation Technologies，Coimbatore，2016，1-6
[9] Avinash Kumar Singh，Sangita Roy. A network-based vulnerability scanner for detecting SQLI attacks in web applications[C]. International Conference on Recent Advances in InformationTechnology (RAIT)，Dhanbad，2012，585-590
[10] M. Yoshimoto，B. B. Bista，T. Takata. Development of security scanner with high portability and usability[C]. International Conference on Advanced Information Networking and Applications(AINA)，2005，407-410
[11] J. L. Lerida，S. M. Grackzy，A. Vina，et al. Detecting security vulnerabilities in remote TCP/IP networks: an approach using security scanners[C]. Annual International Carnahan Conference on Security Technology(CCST)，1999，446-460
[12] Marcelo Invert Palma Salas，Eliane Martins. A Black-Box Approach to Detect Vulnerabilities in Web Services Using Penetration Testing[J]. IEEE Latin America Transactions，2015，707-712
[13] Guo Xiaobing，Qian Depei，Liu Min，et al. Detection and protection against network scanning: IEDP[C]. International Conference on Computer Networks and Mobile Computing，2001，487-493
[14] 维基百科.Scapy[OL].https://zh.wikipedia.org/wiki/Scapy,2019-2-19.
[15] 百度百科.icmp[OL].https://baike.baidu.com/item/ICMP,2020-4-28.
[16] freebuf.经验分享｜谈谈渗透测试中的信息搜集[OL].https://www.freebuf.com/articles/web/179043.html,2018-08-05.
[17] 先知社区.运用Scapy编写类似于Nmap的端口扫描脚本[OL].https://xz.aliyun.com/t/4704,2019-04-09.
[18] 百度百科.服务器端口[OL].https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8%E7%AB%AF%E5%8F%A3#3_11,2020-4-28.
[19] 知乎.Python 实现 FTP 弱口令扫描器[OL].https://zhuanlan.zhihu.com/p/21781496,2016-07-29.
[20] 知乎.初识Scapy--Python的Scapy/Kamene模块学习之路[OL].https://zhuanlan.zhihu.com/p/64008576,2019-04-27.
[21] MENU.Python 实现 SQL 注入检测插件[OL].https://www.wmathor.com/index.php/archives/1191/,2019-02-01.
[22] CSDN.sql注入种类以及测试方式和python脚本[OL].https://

blog.csdn.net/qq_41079177/article/details/89576216,2019-04-26.
[23] 腾讯视频.黑客网络攻防之21端口ftp弱口令爆破[OL].https://v.qq.com/x/page/z0643p2xgth.html,2018-05-03.
[24] CSDN.使用Python打造基本WEB漏洞扫描器(一) 网站爬虫+SQL注入检测[OL].https://blog.csdn.net/qq_41589031/article/details/88315745?depth_1-utm_source=distribute.pc_relevant.none-task-blog-BlogCommendFromBaidu-3&utm_source=distribute.pc_relevant.none-task-blog-BlogCommendFromBaidu-3,2019-03-07.
[25] Scapy.Usage[OL].https://scapy.readthedocs.io/en/latest/usage.html,2020-03-28.
[26] 知乎.渗透&&探测 (之ARP探测篇)[OL].https://zhuanlan.zhihu.com/p/45030189,2018-09-20.
[27] 知乎.渗透&&探测 (之ICMP篇)[OL].https://zhuanlan.zhihu.com/p/44811028,2018-09-18.
[28] （中国）王维波，栗宝鹃，张晓东. Python Qt GUI与数据可视化编程. 人民邮电出版社, 2019.09.
[29] 维基百科.PyQt[OL].https://zh.wikipedia.org/wiki/PyQt,2020-04-09.
[30] CSDN.SQL 注入基础系列3——判断sql注入点[OL].https://blog.csdn.net/weixin_37537965/article/details/85262962?utm_medium=distribute.pc_relevant.none-task-blog-BlogCommendFromBaidu-9&depth_1-utm_source=distribute.pc_relevant.none-task-blog-BlogCommendFromBaidu-9,2018-12-26.
[31] freebuf.Metasploitable2使用指南[OL].https://www.freebuf.com/articles/system/34571.html,2014-05-18.
[32] stackoverrun.Get TCP Flags with Scapy[OL].https://stackoverrun.com/cn/q/5579784,2013-06-13.
[33] Python文档.ipaddress模块介绍[OL].https://docs.python.org/zh-cn/3/howto/ipaddress.html,2020-04-28.
[34] CTOLib码库.IP地址网段表示法总结[OL].https://www.ctolib.com/topics-118046.html,2018-04-20.