

**毕 业 设 计（论 文）开 题 报 告**



**设计(论文)题目：** 安全注册登录的旅游网站

**学生姓名：** \*\*\* **学 号：** \*\*\*\*\*\*\*\*

**专 业：** 信息安全

**所在学院：** 网络安全学院

**指导教师：** \*\*\*\*\*

**职 称：** 副教授

2020 年 11 月 28 日

开题报告填写要求

**1．开题报告（含“文献综述”）作为毕业设计（论文）答辩委员会对学生答辩资格审查的依据材料之一。此报告应在指导教师指导下，由学生在毕业设计（论文）工作前期内完成，经指导教师签署意见及所在专业审查后生效；**

**2．开题报告内容必须用黑墨水笔工整书写或按教务处统一设计的电子文档标准格式打印，禁止打印在其它纸上后剪贴，完成后应及时交给指导教师签署意见；**

**3．“文献综述”应按论文的格式成文，并直接书写（或打印）在本开题报告第一栏目内，学生写文献综述的参考文献应不少于15篇（不包括辞典、手册）；**

**4．有关年月日等日期的填写，应当按照国标GB/T 7408—94《数据元和交换格式、信息交换、日期和时间表示法》规定的要求，一律用阿拉伯数字书写。如“2017年4月26日”或“2017-04-26”。**

**5、开题报告（文献综述）字体请按宋体、小四或五号字体书写，行间距1.5倍（英文字体可采用其它合适的字体，但正文中的英文字体应统一，否则显得凌乱）。**

**6、对每一部分要审清标题，不符合标题的内容不能写入，一定不要把各种材料拿来拼凑某部分的篇幅。**

**7、绝对不能把网上（或书中）材料简单地拷入自己的开题报告（否则一票否决），一定要进行消化整理，用自己的语言，写出相关的内容。**

**8、指称同一概念的名词，全文中使用要统一（如AJAX与Ajax、WEB与Web，只能用其中的一种），以免造成读者的疑问和报告的不规范。**

**9、注意一定用书面语、务必避免口语化倾向，要用客观描述的科技文体，不使用绝对化词语以及夸张的文学词汇及表达，不能有对某种产品的夸张性宣传。**

**毕 业 设 计（论文） 开 题 报 告**

|  |
| --- |
| 1．结合毕业设计（论文）课题情况，根据所查阅的文献资料，每人撰写不少于1500字左右的文献综述： |
| 1. 选题背景和目的   随着人民生活水平的不断提高，嵌入式设备和各种穿戴设备进入人们的生活。加上软件开源潮流不断的涌入，国产操作系统的不懈努力，Linux这类开源操作系统正在不断发展，而这系列嵌入式操作系统和新兴的各种计算机操作系统大多都基于Linux内核。遍布在互联网90%以上的服务器的操作系统都是基于Linux内核的，全球算力前十的超级计算机也都是Linux。可见Linux对计算机与计算机网络影响之大。所以针对Linux平台的安全研究迫在眉睫，Linux系统的安全将会是未来国家信息安全和网络安全的一个趋势。  隐写术，作为在常规CTF中最为简单的比赛项之一，也通常会被比赛选手所忽视。隐写术不单单只是讲重要信息隐藏至某个文件或者某个目录里面，它通常与其他杂项混合在一起，这也是它难度不一的原因，简单的隐写术可以只单单将主要信息隐藏至图片，文本文件中。复杂的情况可以隐写至流量数据包，甚至可执行文件。  本项目在受计算机病毒的启发下，尝试将重要的隐写数据隐藏至可执行文件之中而不破坏程序的正常运行，使其可以像计算机病毒一样工作，使需要隐写的数据寄生至各个可执行文件中，从而防止了隐写数据被破坏，而不像传统隐写术那样简单地将数据存放至图片或者某处。   1. 文献综述 2. 参考文献   [1] Choi, Soojin. Department of Hospitality and Tourism Management, Purdue University等. Destination image representation on the web: Content analysis of Macau travel related websites.[J]. Tourism Management, 2007, Vol.28(1):118-129.  [2]陈衡.Web技术的旅游网站开发与实现[J].现代电子技术,2018,第41卷(7):85-89.  [3] Pi, S.-M.. Web personalization for chinese travel websites(Conference Paper)[J]. Key Engineering Materials, 2011, Vol.474-476(0):1470-1474.  [4] 江雁.浅谈Spring Boot框架下如何快速进行后台开发[J].海峡科技与产业, 2019, (2):131-132.  [5] 杨廷发,兰全祥.基于问题解决的JDBC教学方法改革和探讨[J]. 赤峰学院学报(自然科学版),2018,第34卷(12):148-151.  [6] 范凌云.基于MVVM框架的旅游网站的设计与实现[D].北京交通大学：北京交通大学.2016.  [7] 陈小潘,郑珊珊,朱小柯等.工程教育专业认证背景下Java Web程序设计课程改革与实践探索＊[J].计算机时代,2020,(10):86-88，91.  [8] Teixeira, Leonor1, (lteixeira@ua.pt)Eusébio等. Website accessibility of Portuguese Travel Agents: A view using web diagnostic tools.[J]. CISTI (Iberian Conference on Information Systems & Technologies / Conferência Ibérica de Sistemas e Tecnologias de Informação) Proceedings, 2019, (0):1-7.  [9] 刘小艮.Web前端开发技术及其优化策略[J].信息通信,2020,(10):164-165.  [10] 杨乐,钟文慧,钟添添等.以IT企业需求引导的Web系统开发与设计课程教学内容改革[J].计算机教育,2020,(10):139-143.  [11] 张凡.基于web的旅游服务平台的设计与实现[D].内蒙古大学：内蒙古大学.2018.  [12] 张岚.基于JAVA WEB技术旅游服务网站系统设计与实现[D].电子科技大学：电子科技大学.2012.  [13] 曹青.中国旅游企业电子商务网站评价研究：基于网络链接与网络影响因子测度的分析[J].广东广播电视大学学报,2009,(2)  [14] 王丽丽,吕巍,余娜等.关于内容分析方法对中国旅行社网站营销效果的研究：以国内44家旅行社网站为例[J].上海管理科学,2008,(5):40-47.  [15]华成钢,白长虹,韦鸣秋.移动互联时代旅游信息服务体验对出游决策的影响研究[J].旅游学刊,2019,第34卷(11):51-65.  [16] 马郓,刘譞哲,梅宏.面向移动Web应用的浏览器缓存性能度量与优化\*[J].软件学报,2020,第31卷(7):1980-1996.  [17]李莹,赵瑞,曹宇等.RSA加密算法的研究[J].智能计算机与应用,2020,第10卷(3):166-168. |

**毕 业 设 计（论文） 开 题 报 告**

|  |
| --- |
| 2．本课题要研究或解决的问题和拟采用的研究手段（途径）： |
| 一、本课题研究目标  通过本毕业设计课题的任务，开发出一个基于病毒感染的隐写主程序，通过python脚本转化和提取寄生在可执行文件里面的隐写信息，最后编写脚本来比较提取出来的数据是否与原数据一致。  本设计采用了C语言作为主要语言来编写主要程序，采用部分python和linux shell脚本来辅助主程序的处理。因为程序的开发可能会导致系统的崩溃，所以本次开发均在docker虚拟环境下面进行，所用的操作系统是Ubuntu12.04，开发软件是vim，和make自动化工具。  功能具体描述如下： 1、程序主函数（代码预计100-200行，驱动主要操作）  1.1 使用表单校验（异步提交）  描述：使用stat或fstat，open或fopen，通过Glib对Linux系统调用的封装函数，来检查文件是否存在，隐写程序执行者对需要感染的可执行程序是否拥有可读，‘r’权限，是否可写，如果不满足感染条件，则执行自己编写的错误处理函数，进行相应的处理并且退出程序。  1.2 制作交换文件（程序隐写时所产生的临时文件）  描述：生成新的可执行文件的过程中会产生临时文件进行交换，使用mkstemp函数进行临时文件的创建，并对将可能出现的错误进行处理。  1.3 读取被感染文件信息 (判断文件是否能够被感染)  描述：本项目是面向ELF可执行程序的隐写术，所以我们目前只能隐写至Linux的可执行。ELF可执行文件前EI\_NIDENT个字节里面包含了可执行程序的信息，可以用来判断该可执行文件的文件格式（ELF32 或者 ELF64），通过使用open系统调用读取被感染文件的前EI\_NIDENT个字节来判断该该文件是否是可执行文件，并且判断ELF格式的位数（32 or 64），进而进行下一步的分析，如果发现该文件不是可执行文件则报错退出。    1.4 文件感染  描述：通过上述程序检查，读取要感染的文件，使用Silvio病毒感染算法进行可执行文件的调整，为隐写数据提供足够的空间进行隐藏。   1. 关键技术和难点   1、对于c语言的掌握是一个非常难的点，c语言作为第一门接触的编程语言，通常会被人误以为功能弱小，简单易学的语言。实则不然，深入了解c语言之后才发现，c语言是如此短小而精悍，在很多底层的代码编写中是一门几乎不可能被替代的语言。虽然c语言诞生至今已经大于五十年了，但是从每年的编程语言排行可以看到c语言从古至今几乎一直保持者领先的地位，几乎一直位居前三。c语言解决了第一次软件危机，是所有程序的基石，无论是最底层的网络还是最核心的操作系统内核，绝大部分都是依靠c语言来支撑的。c语言的精华在于其指针，指针又间接指向计算机内存，对c指针的掌握，就拥有了对整个操作系统控制的机会，但是稍不注意就会导致程序崩溃，或者非法修改其他内存。  2、对于Linux ELF文件格式的理解， ELF文件格式经过多年的发展和计算机科学家的不断完善，最终形成了可执行程序中最难理解的文件格式之一，Linux ELF文件格式相对于windows的PE文件格式，添加了延迟绑定，重定位补丁等诸多优化程序性能的功能，这也使得其更加难理解，当然这也是它最有魅力的地方。  3.对于Silvio所提出的text逆向病毒感染算法的理解。Silvio是Unix/Linux 计算机病毒研究的高手，提出了相当多的病毒感染算法，即便是几十年过去，他的算法思想也一直延续至今，我们还能从诸多现代病毒的paper里面看到Silvio的身影。他的算法看似简单，但要实现起来需要相当深厚的c语言基础，c语言的高级编程技巧以及各种数据结构的处理。  三、现有的研究基础  1. 阅读了大量中英文献，对ELF合适比较了解，能够无障碍阅读ELF文件格式的英文文献  2.掌握了C语言、Shell脚本语言、Python语言、ELF文件格式相关数据结构的分析与处理、PE文件格式相关数据结构的分析与处理  3. 了解了二进制文件冷补丁和二进制插桩等高级二进制分析与逆向技术。阅读了关于真实情况下病毒检测和恢复技术，计算机病毒是如果防御反病毒软件的查杀绕过相应的系统保护机制。  四、实施方案  1. 系统技术架构图：  基于病毒感染的隐写术  图 1 系统架构图  这是一个完整的项目，包含完整的C程序源代码，C程序头文件，以及Shell，python等其他语言脚本。C语言完成项目的主要工作，为了考虑程序编写效率，本项目采用Shell和python来处理一些额外的信息。  2.main函数功能模块图  main函数  图 2 main功能模块图  main函数通过argc和argv参数来确定将要寄生的宿主，如果argc小于2，也就是没有指定所需要感染的文件就退出报错，否则进行下一步。  使用操作系统提供的stat系统调用检查被寄生文件是否存在，并且执行者拥有读写权限，如果不存在则退出。  使用open和read系统调用读取ELF可执行文件的固定前几字节，再通过memcmp来比较是否等于ELFMAG，并确定ELF可执行文件的格式类型，后续感染算法会针对32位和64位文件进行相应的修改。  最后做一些守卫工作，使用close来关闭已经打开了的文件，使用free释放内存，使用unlink删除交换文件。  3. infector函数功能模块图  Infector感染器  图 3 infector功能模块图  infector提供文件感染前的处理，这里使用了一些C语言宏代码的技巧，通过判断操作系统的bit数来执行不同的预编译指令，从而能编译出针对不同位数的ELF可执行文件的的感染器。利用BITS(name)##bits指令, 将函数函数命名为相应的位数。  使用check\_elf函数来判断一个elf文件是否合法，并判断其类型。  使用init\_parasite函数，初始化寄生信息（隐写数据），将提取出来的寄生信息复制到内存数组中，整理信息至调转指令之后。  使用infect\_elf函数，找到合适的插入点，调整ELF文件格式，最终将复制数据寄生数据至正常的text段代码之后。   1. 可行性分析   本设计采用的病毒感染算法基于Silov所提出的text段逆向感染算法的修改版本，本算法经前人多年的改进已经变得非常成熟，国外也有很多关于此算法的文章。通过将隐写信息写入 ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked这种可执行文件。因为我熟练掌握ELF文件格式，能够手动patch并写入想要写入的信息，所以，编写这这样的自动化程序虽然有一定难度，但还是可以完成的。 |
|  |

**毕 业 设 计（论文） 开 题 报 告**

|  |
| --- |
| **指导教师意见：** |
| 1．对“文献综述”的评语：  从文献综述来看，该生搜集较多的关于网站开发和旅游有关的相关信息和文献，对于网站开发的应用现状和开发框架都有了较好的掌握和理解，为下一步开展课题研究打下了良好的基础。  2．对本课题的深度、广度及工作量的意见和对设计（论文）结果的预测：  该生基于javaWEB技术开发了一个旅游网站，可为旅游爱好者提供信息服务，具有良好的应用价值，主要涉及密码学、网页开发、数据库等多方面的专业知识，具有一定的深度和广度，工作量适中，应该可以在规定的时间内完成课题。  3.是否同意开题：□同意 □不同意  　　　　　　　　　　　　　　　　指导教师：  202 年 月 日  （时间范围：2020.12.14～12.30，填写完成后删除本行） |
| 所在专业审查意见：  　　　　　　　　　　　　　　　　负责人：  202 年 月 日  （时间范围：2020.12.30～2021.01.10，填写完成后删除本行） |