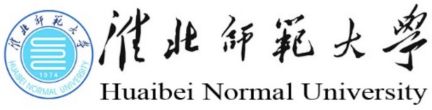

本科毕业论文(设计)

穿“墙”的 Shell 后门设计与实现

学　　院	计算机科学与技术
专　　业	信息安全
研 究 方 向	网络攻防
学 生 姓 名	伍晨旭
学　　号	20151207067
年　　级	2015 级
指导教师姓名	杨忆
指导教师职称	讲师

2019 年 4 月 12 日

穿“墙”的 Shell 后门设计与实现

——————副标题

摘　要: 摘要尽量写成报道性摘要，其内容独立于正文，要能准确、具体、完整地概括原文的创新之处。中文要不少于 200 字，英文摘要应与中文摘要相对应。摘要应回答好以下三个方面问题：1、What you want to do（直接写出研究目的，可缺省）；2、How you did it（详细陈述过程和方法）；3、What results did you get and what conclusions can you draw（全面罗列结果和结论）。中英文摘要一律采用第三人称表述，不使用“本文”、“作者”等作为主语。关键词选词要规范。应尽量从汉语主题词表中选取，未被词表收录的词如果确有必要也可作为关键词选用。中英文关键词应一一对应。

关键词: 关键词 1；关键词 2；关键词 3

Design and Implementation of Shell Backdoor Through Firewall

————Subtitle

Abstract: As far as possible, it should be written as a report summary, whose content is independent of the text, and it should be able to accurately, concretely and completely summarize the innovations of the original text. Chinese abstracts should be no less than 200 words. English abstracts should correspond to Chinese abstracts. The following three questions should be answered well: 1. What do you want to do (write the research purpose directly, but default); 2. How did you do it (state the process and method in detail); 3.What results did you get and what conclusions can you draw. Both Chinese and English abstracts are expressed in the third person without the use of ”the text” or ”the author” as the subject.

Key words: keyword1;keyword2;keyword3

目　录

绪论 1

1 特洛伊木马的现状 2

1.1 木马的定义 2

1.2 木马的特点 2

1.3 新型木马的意义 2

1.3.1 新型木马优点 2

1.3.2 新型木马缺点 2

2 防火墙技术 3

2.1 状态监测防火墙 3

2.2 包过滤防火墙 3

2.3 应用型防火墙 3

2.4 防火墙实例 4

2.4.1 Netfilter 框架结构 4

2.5 Netfilter 包过滤原理 5

2.6 制定防火墙策略 5

3 TDShell 的工作原理与分析 6

3.1 连接参数配置函数的工作原理和实现 6

3.2 数据处理函数的工作原理和实现 6

3.3 主函数的工作原理与实现 7

4 服务端功能的实现 8

4.1 连接参数配置函数的工作原理和实现 8

4.2 数据处理函数的工作原理和实现 8

4.3 主函数的工作原理与实现 9

5 客户端原理与实现 10

5.1 连接服务器函数的工作原理和实现 10

5.2 退出及自毁函数的工作原理与实践 10

5.3 处理服务端命令函数工作原理和实现 10

6 测试与使用 11

6.1 Linux 环境下测试 11

6.1.1 服务器端 11
6.1.2 客户端 11
6.2 MAC OS 环境下测试 11
6.2.1 服务器端 11
6.2.2 客户端 11
6.3 Windows 环境下测试 11
6.3.1 服务器端 11
6.3.2 客户端 11
7 总结 12
7.1 工作总结 12
7.2 进一步研究方向 12
参考文献 13
附录 A 14
致谢 15

绪论

从上世纪五十年代苏联第一次发射人造卫星开始，互联网经过大半个世纪的快速发展，伴随着电脑进入了千千万万家庭的家中，同时进入家庭的还有诸多虚拟空间的安全隐患。在 2018 年 9 月，互联网互联网恶意程序排名中，后门占 11.5%[1]，位居第四，成为网络安全领域中不得不关注和防范的一类恶意代码程序。

后门作为一种典型的特洛伊木马，

1 特洛伊木马的现状

1.1 木马的定义

为了使用该模板，需要安装一个 TeX 的发行版本。可以选择 Texlive 或者 Miktex, 他们都是跨平台的。而 Texlive 打包了比较多的宏包，较为庞大，Miktex 则是临时下载没有的宏包。这里我推荐使用 Miktex。但是对于 Mac，推荐使用 MacTeX，它是为 Mac 定制的发行版本，应该比较合适。特别提醒 CTeX 套装无法运行该模板。关于编译方式需选择 XeLaTeX, 否则无法正常编译该模板。

1.2 木马的特点

为了正确使用该模板，请按照提示安装好可使用的 TeX 发行版本。因为论文内容比较多，因此采取了分文件的方式来构成该文档。主文档 hbnuthesis.tex 的位置位于 Main 下，正确编译后所得的 pdf 文件就在这里。Figure 文件夹是存放图片的文件夹，该文件夹已经加入图片文件夹的位置，插入图片是无需多加路径，直接用文件名即可。关于 Setting 文件夹只需要把里面的 Information.tex 正确填入即可。而你需要编辑的仅有 Body 文件夹下的文件。

该模板是在厦门大学博士学位论文模板的基础上修改得到的。由于本人水平有限，因此该模板写的并不好，但是应该勉强能够满足毕业论文的要求。但是仍然可能有许多错误的地方，希望各位使用者如果能发现错误之处能够提出。可以给我法邮件或者直接在 github 上面提 issue。欢迎大家的参与，共同完善母校的模板。

1.3 新型木马的意义

由于本人是一名理科生，对文科的同学毕业论文的额外需求可能了解不多。虽说文科生用这个模板的可能性比较小，如果有人用，有额外的需求也可以提出。

1.3.1 新型木马优点

1.3.2 新型木马缺点

联系方式：邮箱：tdhypocrites@163.com

github 项目的地址: HBNU-Undergraduate-thesis-template

2 防火墙技术

毕业论文 (设计) 用 A4 纸单面打印。版面页边距上、下、左、右各 2.5cm; 封面不编页码; 从摘要页开始，摘要和目录连续标注页码，页码为罗马数字，用 Times New Roman、小五号字放页面底端居中; 论文正文从首页开始标注页码，页码为阿拉伯数字，用 Times New Roman、小五号字放页面底端居中。[1]

2.1 状态监测防火墙

- 科学技术名词术语采用全国自然科学名词审定委员会公布的规范词或国家标准、部标准中规定的名称，尚未统一规定或有争议的名词术语，可采用惯用的名称。
- 特定含义的名词术语或新名词、以及使用外文缩写代替某一名词术语时，首次出现时应在括号内注明其含义，如：OECD（Organization for Economic Co-operation and Development）代替经济合作发展组织。
- 外国人名一般采用英文原名，可不译成中文，英文人名按名前姓后的原则书写。一般很熟知的外国人名 (如牛顿、爱因斯坦、达尔文、马克思等) 可按通常标准译法写译名。

2.2 包过滤防火墙

- 论文中某一物理量的名称和符号应统一，一律采用国务院发布的《中华人民共和国法定计量单位》或者国际公认的计量单位。单位名称和符号的书写方式，应采用国际通用符号。
- 在不涉及具体数据表达时允许使用中文计量单位如“千克”。
- 表达时间使用“2014 年 6 月”，不能使用“14 年 6 月”或“2014.6”。不能使用 80 年代，而应为上世纪 80 年代或 20 世纪 80 年代。表达时刻应采用中文计量单位，如“下午 3 点 10 分”，不能写成“3h10min”，在表格中可以用“3:10PM”表示。
- 物理量符号、物理量常量、变量符号用斜体，计量单位符号均用正体。

2.3 应用型防火墙

1. 无特别约定情况下，一般均采用阿拉伯数字表示。
2. 小数的表示方法：一般情形下，小于 1 的数，需在小数点之前加 0。但当某些特殊数字不可能大于 1 时（如相关系数、比率、概率值），小数点之前的 0 可去掉，如 $r = .26, p < .05$ 。
3. 统计符号的格式：一般除 $\alpha, \beta, \lambda, \epsilon$以及$V$ 等符号外，其余统计符号一律以斜体字呈现，如 *ANCOVA*，*ANOVA*，*MANOVA*，*N*，*nl*，*M*，*SD*，*F*，*p*，*r* 等。

[1]以上内容仅供参考，详见《计算机科学与技术学院本科毕业论文（设计）撰写规范 201805》

2.4 防火墙实例

1. 公式应另起一行缩略书写，居于中央（注意行首无缩进），与周围文字留足够的空间区分开。

2. 公式的编号用英文圆括号括起，放在公式右边行末，在公式和编号之间不加虚线。子公式可不编序号，需要引用时可加编 a、b、c……，重复引用的公式不得另编新序号。公式较多时，可分章编号，但应与表格、图的编序方式统一。

3. 较长的公式最好在等号处转行，或在运算符号（如“+”、“-”号）处转行，等号或运算符号应在转行后的行首。公式中分数线的横线，其长度应等于或略大于分子和分母中较长的一方。

$$1+1=2 \tag{2.1}$$

公式 (2.1) 是大家所熟知的。我们可以用这两种方式进行引用：\cref{eq1} 和 \eqref{eq1}，两种都可以。

不想要编号的公式就用这样的方式：

$$2\times 2=4$$

行内公式就是 $\alpha^2=\beta$

2.4.1 Netfilter 框架结构

$$\begin{aligned} a &= b+c && (2.2)\\ &= d+e+f+g+h+i+j+k+l \\ &\quad +m+n+o && (2.3)\\ &= p+q+r+s && (2.4) \end{aligned}$$

$$\begin{aligned} a &= b+c \\ d &= e+f+g \\ h+i &= j+k \\ l+m &= n \end{aligned} \tag{2.5}$$

定理 2.4.1 (Energy–momentum relation)**.** *The relationship of energy, momentum and mass is*

$$E^2=m_0^2c^4+p^2c^2$$

where c is the light speed.

定律 2.4.1. Don't hide in the witness box.

证明. For simplicity, we use

$$E = mc^2$$

That's it. □

2.5 Netfilter 包过滤原理

这是算法的插入示例，可能软件学院、信息科学学院这类的同学用得上吧。

Algorithm 1 My algorithm

```
1:  procedure MyProcedure
2:      stringlen ← length of string
3:      i ← patlen
4:  top:
5:      if i > stringlen then return false
6:      j ← patlen
7:  loop:
8:      if string(i) = path(j) then
9:          j ← j − 1.
10:         i ← i − 1.
11:         goto loop.
12:         close;
13:     i ← i + max(delta_1(string(i)), delta_2(j)).
14:     goto top.
```

2.6 制定防火墙策略

1. 表格要有：表号，表名，单位。表号和表名居表上方正中（注意行首无缩进）；表格只有一个单位时，单位在表右上方。表较多时，可分章编号，但须与插图、公式的编序方式统一。

2. 表格应优先采用三线表，三线表头尾两条线宽 1 磅，中间线宽 0.75 磅。也可根据需要使用其他格式。

3. 表格如参考其他资料，应标明“作者、来源名称、时间”，置表格左下方。

4. 表格允许下页接写，接写时应重复表号，表号后跟表名（可省略）和“（续）”，置于表上方。续表应重复表头。

5. 表格应放在离正文首次出现处最近的地方，不应超前和过分拖后。表与上下正文之间各空一行。

3 TDShell 的工作原理与分析

毕业论文 (设计) 一般由以下部分组成:[?]

毕业论文 (设计) 封面;

诚信承诺书;

中英文摘要;

目录;

正文;

参考文献;

附录;

致谢;

成绩评定表;

答辩记录;

论文相似性鉴定报告首页。

3.1 连接参数配置函数的工作原理和实现

由学生本人亲自用黑色水笔手写签订《淮北师范大学本科生毕业论文 (设计) 诚信承诺书》。诚信承诺书内容见校教字 [2013]67 号文的附件 5。

3.2 数据处理函数的工作原理和实现

摘要是论文内容的简要陈述，应尽量反映论文的主要信息，内容包括研究目的、方法、成果、结论及主要创新之处等，不含图表，不加注释，具有独立性和完整性。中文摘要不少于 200 字，英文摘要应与中文摘相对应，且中文摘要在前，英文摘要在后。中文摘要和英文摘要均要另起一页。

关键词是反映毕业设计 (论文) 主题内容的名词，是供检索使用的。中英文摘要均要有关键词，关键词一般为 3-5 个，各关键词用分号隔开。关键词排在摘要正文部分下方。

中文摘要页中，论文主标题样式用二号、黑体、居中，单倍行距，段前 12 磅，段后 6 磅; 若有子标题，子标题样式用四号、宋体、加粗，右对齐，右侧缩进 4 字符，单倍行距，段前 0 磅，段后 24 磅。论文标题排在摘要之前。

中文摘要标题“摘要”和“关键词”几个字样式用小四、黑体、加粗、顶格，中文摘要正文样式用小四、宋体、行距固定值 20 磅 (注: 行间距 12 磅为 1 行，下同)。摘要标题后紧接写摘要正文 (不另起一行)。中文关键词样式用小四、宋体、行距固定值 20 磅。

英文摘要页中，论文主标题样式用二号、Arial、加粗、居中，单倍行距，段前 12 磅，段后 6 磅; 若有子标题，子标题样式用四号、Arial、加粗，右对齐，右侧缩进 4 字符，单倍行距，段前 0 磅，段后 24 磅。主标题和子标题的第一个词和所有实词首字母大写，虚词首字母小写。

英文摘要标题“Abstract”和“Key words”几个字样式用小四、Times New Roman、加粗、顶格，英文摘要正文样式用小四、Times New Roman，两端对齐，行距固定值 20 磅。每个英文关键词首字母要大写，样式用小四、Times New Roman，行距固定值 20 磅。

3.3 主函数的工作原理与实现

目录按三级标题编写，要求层次清晰，且要与正文标题一致。主要包括绪论 (或引言)、正文主体、结论 (或总结)、参考文献、附录及致谢等。“目录”二字样式用小三号、黑体、加粗、居中，单倍行距，段前 0 磅，段后 12 磅，“目”与“录”之间空四格。目录内容中文样式用宋体，英文样式用 Times New Roman。字号、行间距自行统一样式。目录要另起一页。

4 服务端功能的实现

毕业论文 (设计) 一般由以下部分组成:[?]

毕业论文 (设计) 封面;

诚信承诺书;

中英文摘要;

目录;

正文;

参考文献;

附录;

致谢;

成绩评定表;

答辩记录;

论文相似性鉴定报告首页。

4.1 连接参数配置函数的工作原理和实现

由学生本人亲自用黑色水笔手写签订《淮北师范大学本科生毕业论文 (设计) 诚信承诺书》。诚信承诺书内容见校教字 [2013]67 号文的附件 5。

4.2 数据处理函数的工作原理和实现

摘要是论文内容的简要陈述，应尽量反映论文的主要信息，内容包括研究目的、方法、成果、结论及主要创新之处等，不含图表，不加注释，具有独立性和完整性。中文摘要不少于 200 字，英文摘要应与中文摘相对应，且中文摘要在前，英文摘要在后。中文摘要和英文摘要均要另起一页。

关键词是反映毕业设计 (论文) 主题内容的名词，是供检索使用的。中英文摘要均要有关键词，关键词一般为 3-5 个，各关键词用分号隔开。关键词排在摘要正文部分下方。

中文摘要页中，论文主标题样式用二号、黑体、居中，单倍行距，段前 12 磅，段后 6 磅; 若有子标题，子标题样式用四号、宋体、加粗，右对齐，右侧缩进 4 字符，单倍行距，段前 0 磅，段后 24 磅。论文标题排在摘要之前。

中文摘要标题“摘要”和“关键词”几个字样式用小四、黑体、加粗、顶格，中文摘要正文样式用小四、宋体、行距固定值 20 磅 (注: 行间距 12 磅为 1 行，下同)。摘要标题后紧接写摘要正文 (不另起一行)。中文关键词样式用小四、宋体、行距固定值 20 磅。

英文摘要页中，论文主标题样式用二号、Arial、加粗、居中，单倍行距，段前 12 磅，段后 6 磅; 若有子标题，子标题样式用四号、Arial、加粗，右对齐，右侧缩进 4 字符，单倍行距，段前 0 磅，段后 24 磅。主标题和子标题的第一个词和所有实词首字母大写，虚词首字母小写。

英文摘要标题“Abstract”和“Key words”几个字样式用小四、Times New Roman、加粗、顶格，英文摘要正文样式用小四、Times New Roman，两端对齐，行距固定值 20 磅。每个英文关键词首字母要大写，样式用小四、Times New Roman，行距固定值 20 磅。

4.3 主函数的工作原理与实现

目录按三级标题编写，要求层次清晰，且要与正文标题一致。主要包括绪论 (或引言)、正文主体、结论 (或总结)、参考文献、附录及致谢等。“目录”二字样式用小三号、黑体、加粗、居中，单倍行距，段前 0 磅，段后 12 磅，“目”与“录”之间空四格。目录内容中文样式用宋体，英文样式用 Times New Roman。字号、行间距自行统一样式。目录要另起一页。

5 客户端原理与实现

5.1 连接服务器函数的工作原理和实现

论文中汉字应采用《简化汉字总表》规定的简化字，并严格执行汉字的规范。所有文字字面清晰，不得涂改。

5.2 退出及自毁函数的工作原理与实践

论文的表格逐章单独编号 (如: 如第 2 章第 3 个表编号为: 表 2-3)，表编号必须连续，不得重复或跳跃。表编号和表名称置于表格上方，样式用五号、宋体、居中，单倍行距; 表中文字中文样式用五号、宋体，英文样式用五号、Times New Roman; 整个表居中对齐。

表格的结构应简洁。表格中各栏都应标注量和相应的单位。表格内数字须上下对齐，相邻栏内的数值相同时，不能用‘同上’、‘同左’和其它类似用词，应一一重新标注。

5.3 处理服务端命令函数工作原理和实现

论文的图逐章单独编号 (如: 如第 3 章第 4 个图编号为: 图 3-4)，图编号必须连续，不得重复或跳跃。图编号和图名称置于图下方，样式用五号、宋体，单倍行距。整个图居中对齐。

插图要精选。毕业论文 (设计) 中的插图以及图中文字符号应打印，无法打印时一律用钢笔绘制和标出。

由若干个分图组成的插图，分图用 a,b,c,..... 标出。

6 测试与使用

6.1 Linux 环境下测试

6.1.1 服务器端

6.1.2 客户端

6.2 MAC OS 环境下测试

6.2.1 服务器端

6.2.2 客户端

6.3 Windows 环境下测试

6.3.1 服务器端

6.3.2 客户端

7 总结

7.1 工作总结

7.2 进一步研究方向

参考文献

[1] 国家互联网应急中心. 计算机恶意程序传播渠道安全检测报告-2018 年 9 月[J/OL]. 网络安全, 2018. http://www.cert.org.cn/publish/main/upload/File/2018%2009%20malware%20.pdf.

下面是一个 Matlab 的代码的插入，还可以插入其它类型的代码。有额外需求可以添加。

```
clc; close all; clear all;
[X,Y]=meshgrid(-8:0.3:8);
R=sqrt(X.^2+Y.^2)+eps;
Z=sin(R)./R
surf(X,Y,Z);
colormap; colorbar;
xlabel('X␣Axis');
ylabel('Y␣Axis');
zlabel('Y␣Axis');
```

附录里面还可以放其它需要的内容，它们是文章的补充。

致谢

致谢语应以简短的文字对课题研究与论文撰写过程中曾直接给予帮助的人员 (例如指导教师、答疑教师及其他人员) 表示自己的谢意。

谢辞应以简短的文字对在课题研究和论文撰写过程中曾直接给予帮助的人员 (例如指导教师、答疑教师及其他人员) 表示自己的谢意，这不仅是一种礼貌，也是对他人劳动的尊重，是治学者应有的思想作风。“致谢”二字样式用小三、黑体、加粗、居中，单倍行距，段前 6 磅，段后 12 磅。内容限 1 页，采用小四、楷体 _GB2312，行距固定值 20 磅。致谢要另起一页。第一部分可以简述论文写作的经历，所面对的挑战以及你如何应对。第二部分具体感谢在论文过程中给与你帮助的人。第三部分指出你将为自己的论文承担责任，如果你希望将此论文献给谁，可以在最后指出。致谢内容请亲自撰写，使其具备你个人的特色。抄袭任何模板内容是极其懒惰、没有意义、不负责任和错误的行为。