# 开题报告

**一、选题意义**

随着网络技术的发展,网络作为一种传递各种信息的媒介，网络泄密事件时有发生，网络信息传输安全越来越受到重视。各种网络攻击层出不穷，已经严重的影响到互联网的发展，作为对计算机安全影响甚大的木马类程序尤为恶劣。木马能在计算机上执行窃听以及控制功能，一旦计算机被植入恶意代码，就会造成重要文件和信息的窃取以及一切操作行为被监视的后果。但是由于现在越来越多的恶意代码开始利用隐蔽通信技术来绕过安全系统的检测和过滤，使木马客户端和服务器端的通信具有高隐蔽性，更难被检测到。

现有的木马隐蔽通信技术通常有如下几种思想方法：隐藏于已存在的通信量中；利用常规协议的源和目的端口，如端口复用技术；通过加密或者隐写技术不以明文传送数据；使用内核层 Rootkit 技术隐蔽通信；基于 NDIS 中间层驱动的隐蔽通信技术。在这些实现中，端口隐藏技术是木马常用的关键隐藏技术之一，用来实现服务端与控制端通信通道的隐藏。

攻击与防御是相互对立的，研究攻击技术是为了能够在防御中占据主动权。木马隐蔽通信技术作为隐蔽通信的典型，研究木马在隐蔽通信中的技术变得越来越重要。本次毕业设计主要研究在木马通信这一特定情景下的隐蔽通信，并且主要以端口隐藏的方式实现隐蔽通信技术。

**二、国内外研究现状概述**

针对木马隐蔽通信技术的研究现状

随着人们对计算机的依赖性越来越高，信息越来越多地在网络上传输，用户文件信息被盗时有发生，对这类安全事件影响尤为恶劣的木马隐蔽通信已经成为网络安全的一个重要研究热点。

在对木马隐蔽通信技术的研究中，文献[1]提到利用已存在的通信流量隐藏木马通信的技术，也就是协议域隐蔽通信技术。常见的协议利用技术有如下几种：

域名系统 (DNS)隐蔽通道，通过修改 DNS协议请求报文， 添加木马程序的通信数据到 DNS 报文中； Internet控制报文协议 (ICMP)隐蔽通道，将木马程序的通信数据隐藏在 ICMP 报文格式的选项数据字段进行传送；超文本传输协议(HTTP)隐蔽通道，将HTTP正常流量作为背景流量，在通信过程中嵌入隧道流量，实现对目标主机的恶意攻击行为。文献[2]提出了几种http协议上的几种新的应用层隐蔽信道，通过冗余性研究在HTTP协议上发现了5种新的隐蔽通道，但是隐蔽通道都是原始的，对秘密信息没有经过隐写伪装、纠错编码、变形加密等流程，通道的透明性差、不能抵抗基于统计方法及机器学习方法的隐写分析。

针对端口隐藏技术的研究，文献[4]针对用户级的端口复用提出了内核级别的端口复用。该技术采用复用已开放端口，可以顺利穿过防火墙，巧妙地利用了 T D I 层截获网络数据包、采用共享内存和事件通知实现应用程序和驱动通信等方法，避免了在受控端开启监听端口和反弹连接所带来的一系列问题，并且较好地解决了通信的可靠性。

针对通过加密或者隐写技术不以明文传送数据的研究，文献[10]系统地描述了基于网络协议隐写传输信息的方法，并给出了相应的对抗策略，然而通过隐写的隐藏手段并不能躲避本地抓包工具的分析．

现在越来越多的木马程序开始利用内核层Rootkit技术来实现隐蔽通信。但是随着 RootKit 技术和反 RootKit 技术的不断发展和交替进步，木马的隐蔽通信技术逐渐扩展到操作系统的核心态和底层，出现了另外一种Rootkit 隐蔽通信技术，开发自定义的网络驱动接口规范(NDIS) 协议驱动而不使用传输控制协议 / 因特网互联协议 (TCP/IP) 协议栈来传输据，从而躲避检测系统对通信数据的捕获。文献[11]提出了一种基于NDIS驱动的木马隐蔽通信技术，木马的通信模块位于 Windows 网络结构底层，在防火墙截获主机网络通信数据之前对其进行 分流处理，将木马通信数据直接与木马的功能模块交互。从而，防火墙没有机会接触到木马通信数据，达到了绕过防火墙进行隐蔽通信的目的。NDIS 驱动程序位于 Windows 网络通信结构(不包含物理层)的最底层。在上文给出的木马验证模型中，木马通信数据受 NDIS 驱动程序控制直接经由网卡发送和接收，不会经过应用程序、Windows API、SPI、TDI 等层次。因此，可以推断防火墙的用户态网络数据包拦截方法、TDI 过滤驱动程序拦截方法、Win2k Filter-Hook Driver 拦截方法无法截获木马通信数据。

由此可见，即使检测技术在不断更新改进，但是木马隐蔽通信技术同样也在不断发展，不断深入底层，使得现有的检测技术难以满足网络安全的需求，研究木马隐蔽通信技术是为以后的检测以及隐蔽通信技术的良好应用打下更好的基础。

**三、主要研究内容**

本文主要研究内容主要有：

1. 对主要的木马隐蔽通信技术进行研究

现在的隐蔽通信技术虽然已经取得了一定研究成果，但是仍然存在易被检测以及性能较低等问题。而一个完整的木马程序基本要求就是要实现隐藏、反检测以及反跟踪能力，就木马发展至今而言，高隐藏性已经成为木马的一大特征，其隐藏性主要针对木马本体文件、模块文件、通讯端口三个方面，所以我们研究现今主要的木马隐蔽通信技术，为隐蔽通信技术的良好实现以及针对木马的检测打下良好的基础。文献[15]提出木马隐蔽通信技术具体来说可以分为真隐藏和假隐藏，真隐藏是通过技术手段，使用户无法通过工具，如netstat命令查看通信端口，假隐藏是指端口还在，只是使用户误认为是正常端口，如端口复用技术。本文总结并比较了几种木马隐蔽通信技术，其中既包含了真隐藏，也包含了假隐藏。

1. 研究并设计实现一种新的端口隐藏技术

木马隐藏技术中，对通讯端口的隐藏是一大方面。为了研究发掘现存的端口隐藏技术的缺陷，本文的第二个工作就是研究并设计实现一种新的端口隐藏技术。大多数木马都是用TCP通讯，这样就会有一个控制端与被控端之间维持的TCP连接，为了起到木马本体的隐藏效果，这个端口是必须要隐藏的。当然我们可以直接不使用端口，比如使用其他协议如ICMP协议，但是木马就需要自己确保数据包完整到达并且实现一系列的协议等。现存的端口隐藏技术主要有以下几个方法：

1. 直接修改跳转地址的挂钩技术，如SSDT Hook，IAT Hook，IRP Hook技术；
2. 修改代码段执行顺序的挂钩技术，如Inline Hook；
3. 利用TCP/IP协议中的冗余字段来构造数据包；
4. 端口复用，在windows实现winsock时，在端口上进行通信，只是根据输入的信息进行最明确的匹配；
5. 过滤驱动技术，通过添加新的过滤程序，可以捕获到当前I/O栈所在的设备对象发送的所有IRP请求，通过修改请求内容或者修改请求结果实现隐藏功能。比如基于NDIS中间层驱动技术的隐蔽通信技术可以直接截获来自网络适配器来的数据包，取得对各层次协议的完全控制。

**四、拟采用的研究思路（方法、技术路线、可行性论证等）**

1)针对几种木马隐蔽通信方式的实现层、实现方法、相应的检测技术来对其进行比较，发现总结其优点及缺陷。

2)在现存的端口隐藏技术的基础上进行研究改进，设计实现一种新的端口隐藏的方式

3) 通过在各大防火墙环境下测试该方案的可行性、隐蔽性等

**五、研究工作安排及进度**

2019年9月29日-2019年11月7日：接受毕业论文任务

2019年11月8日-2019年11月20日：阅读参考文献，准备论文开题

2019年11月21日-2019年11月23日：论文开题，完成开题报告

2019年11月24日-2020年12月15日：阅读文献，调研，英文文献翻译

2020年12月16日-2020年1月20日：进行系统架构设计

2020年1月21日-2020年2月31日：核心技术的研究与编程实现

2020年3月1日-2020年3月31日：系统测试，确定论文框架结构

2020年4月1日-2020年4月20日：完成论文初稿

2020年4月21日-2020年4月26日：整理材料，修改论文，准备答辩

**六、参考文献目录**

[1] 赵琦,蒋朝惠,周雪梅,宋紫华.一种基于HTTP协议的隐蔽隧道及其检测方法[J].计算机与现代化,2019(06):16-23+29.

[2]马文岩． HTTP 协议上几种新的应用层隐蔽通道［J］．计算机光盘软件与应用，2014，17( 15) : 179-180．

[3]罗改龙,程胜利.基于端口复用技术的木马研究[J].计算机工程,2007(15):165-166+169.

[4]何乐. 内核级端口复用技术的研究和实现[A]. 中国通信学会青年工作委员会.2006通信理论与技术新进展——第十一届全国青年通信学术会议论文集[C].中国通信学会青年工作委员会:中国通信学会青年工作委员会,2006:5.

[5]Sohn T, Moon J, Lee S, et al. Covert channel detection in the ICMP payload using support vector machine[C]//International Symposium on Computer and Information Sciences. Springer, Berlin, Heidelberg, 2003: 828-835.

[6]Johnson D, Yuan B, Lutz P, et al. Covert channels in the HTTP network protocol: Channel characterization and detecting man-in-the-middle attacks[J]. 2010.

[7]王传安．基于信息熵 SVM 的 ICMP 隐蔽通道检测研究［D］． 镇江: 江苏大学，2009．

[8]强亮，李斌，胡铭曾． 基于 HTTP 协议的网络隐蔽通道研究［J］． 计算机工程，2005( 15) : 224-225．

[9]张臣,王轶骏,薛质.基于客户端蜜罐的木马隐蔽通信检测[J].信息安全与通信保密,2011(02):49-51.

[10]Zander S, Armitage G, Branch P. A survey of covert channels and countermeasures in computer network protocols[J]. IEEE Communications Surveys & Tutorials, 2007, 9(3): 44-57.

[11]杨志程,舒辉,董卫宇.基于NDIS隐蔽通信技术的木马病毒分析[J].计算机工程，2008(10):147-149.

[12]王全民. 基于NDIS的端口隐藏检测技术[A]. 中国通信学会.第十八届全国青年通信学术年会论文集（上册）[C].中国通信学会:中国通信学会,2013:5.

[13]王永杰，刘京菊.基于DNS 协议的隐蔽通道原理及性能分析［J］．计算机工程，2014，40( 7) : 102-105．

[14]Hoglund G, Butler J. Rootkits: subverting the Windows kernel[M]. Addison-Wesley Professional, 2006.

[15]贺毅. 基于P2P的木马隐藏技术研究与实现[D].西安理工大学,2016.