**选题目的、工作任务：**

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。

**目前资料收集情况：**

基于木马的计算机远程控制及隐藏技术研究

基于P2P的木马隐藏技术研究

基于客户端蜜罐的木马隐蔽通信检测

Rootkit实现端口隐藏

<https://github.com/Cos4Nostr4/Praktikum-2.git>

[利用端口复用技术隐藏后门端口](https://www.cnblogs.com/PeterZ1997/p/9532045.html)

<https://www.cnblogs.com/PeterZ1997/p/9532045.html>

**完成计划（含时间进度）：**

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