****

网络安全理论与技术课程设（乙）

软件安全及防火墙实验

实 验 报 告

|  |  |  |  |
| --- | --- | --- | --- |
| **学 院** | 网络空间安全学院 | | |
| **专 业** |  | | |
| **班 级** |  | | |
| **学 号** |  | | |
| **学生姓名** |  | | |
| **教师姓名** | 陈黎丽 | | |
| **完成日期** |  | | |
| **成 绩** |  | | |
| **组长/组员姓名** | | **学号** | **报告分工** | |
|  | |  |  | |
|  | |  |  | |
|  | |  |  | |
|  | |  |  | |
| **目录（自动生成，引用可生成）** | | | | |
| **软件安全及防火墙实验** | | | | |
| **实验目的**  1、深入理解防火墙的原理、部署  2、通过恶意代码的静态检测和动态检  3、学习软件安全防护的原理，获取检测恶意代码的方法。 | | | | |
| **实验任务**  1、自行搭建主机防火墙  2、通过对恶意代码的行为日志数据的观察，将将病毒具体的恶意行为与之进行关联，了解恶意代码运行的基本信息  **扩展功能：**实现软件代码第三方库的漏洞检测、模拟攻击、流量获取、特征提取。（任选一种也可以） | | | | |
| 一、必做题实验任务1（搭建主机防火墙）（学生1，学生2）实验任务  * 启动并查看iptables，查看iptables 的所有链和规则，默认的是filter表 * 清除掉所有的默认规则 * 把规则加到INPUT链上，适用于所有TCP包，允许目标端口22对应的SSH，以及80端口对应的web * 禁止10.0.0.0/24 网段连入 * 禁止23端口 * 允许DNS查询回复 * 禁止ICMP协议类型 * 查看所有配置 * 在另一台主机上使用telnet连接（连接不上，对应端口23）、ssh连接（能连接上，对应端口22）以及ping（连接不上）测试  实验原理 Netfilter/iptables (以下简称iptables)是nuix/linux 系统自带的优秀且完全免费的基于包过滤的防火墙工具、它的功能十分强大、使用非常灵活、可以对流入、流出及流经服务器的数据包进行精细的控制。 实验环境 Ubuntu或者Kali，系统自带iptables，如果没有请自己安装。 实验过程及结果分析实验问题及解决1.1.6 实验总结实验任务2（恶意代码的静态检测与动态检测）（学生3）实验任务  * 从网上下载勒索病毒或者其他病毒文件，根据病毒的运行环境要求安装虚拟机环境（比如，勒索病毒WannaCry 运行的系统环境是win7），在虚拟机上运行病毒； * 根据参考资料（1）安装Process Monitor、PCHunter或者火绒剑、wireshark，在病毒运行过程中，使用工具记录病毒的行为数据，包括API、注册表、文件操作、网络连接、网络流量等，保存成日志文件； * 将病毒具体的恶意行为与行为日志数据具体关联起来。 * 使用[PEID](https://www.52pojie.cn/thread-12865-1-1.html)或者其他工具，静态查看病毒文件的基本信息，包括是否加壳、PE信息、DLL信息、API信息等； * 将静态行为和动态行为联合分析病毒的恶意行为。  实验环境 根据病毒的运行环境要求安装虚拟机环境，如，勒索病毒WannaCry 运行的系统环境是win7），在虚拟机上运行病毒； 实验过程及结果分析实验问题及解决实验总结二、选做题（学生4） **2.1.1 实验任务** 2.1.2实验原理2.1.3 实验环境2.1.4 实验过程及结果分析2.1.5实验问题及解决2.1.6 实验总结 | | | | |