实验：学习软件安全及防火墙实验

任务 1：必做题

任务 1.1：搭建主机防火墙

（1）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。

相关参考资料：http://www.zsythink.net/archives/1199

（2）实验环境

Ubuntu 或者 Kali，系统自带 iptables，如果没有请自己安装。

（3）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
-

提示：本实验配置完之后，请输入命令 ~#iptables save </etc/iptables.rules 保持配置的命令文件，否则，下次开机的时候会发现配置的命令没有了

参考资料：https://www.cnblogs.com/liang2580/articles/8400140.html

任务 1.2：恶意代码的静态检测和动态检测

（1）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；

（2）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；

（3）将病毒具体的恶意行为与行为日志数据具体关联起来。

（4）使用 PEID 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；

（5）将静态行为和动态行为联合分析病毒的恶意行为。

参考资料：
勒索病毒下载：https://wwwz.lanzouo.com/iR6E8yl1yuf
Process Monitor 安装使用：https://blog.csdn.net/zoulisheng2011/aritcle/details/124858491
勒索病毒分析参考：https://www.52pojie.cn/thread-1573058-1-1.html

任务 2：选做题

任务 2.1 软件代码第三方库的漏洞检测

（1） 从 github 上下载一个 Web 网站的代码，或者自己之前编写的网站代码；

（2） 查看代码中调用了哪些第三方库；

（3） 从 nvd、cve、exploit-db、cnvd、cnnvd 等国内外著名的漏洞网站上，获取这些第三方库的漏洞名称、编号、危害等级、类型、发布时间、威胁类型、厂商、简介/修复建议等信息

（4） 根据漏洞特征、判断软件调用的第三方库是否存在漏洞；如果存在漏洞，根据漏洞详情，提供修复建议。

任务 2.2 模拟攻击、流量获取、特征提取

（1）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，在虚拟机上运行病毒；

（2）使用 wireshark 或者 tcpdump 抓包，保存成 pcap 包；

（3）根据参考资料（1）安装 CICFlowMeter，从 pcap 包中提取流量特征，保存到 csv 文件中；

参考资料：
勒索病毒下载：https://wwwz.lanzouo.com/iR6E8yl1yuf
（1）https://blog.csdn.net/qq_40004550/article/details/103633684