高老师实验安排

一、实验内容

- 初级（0~60 分）

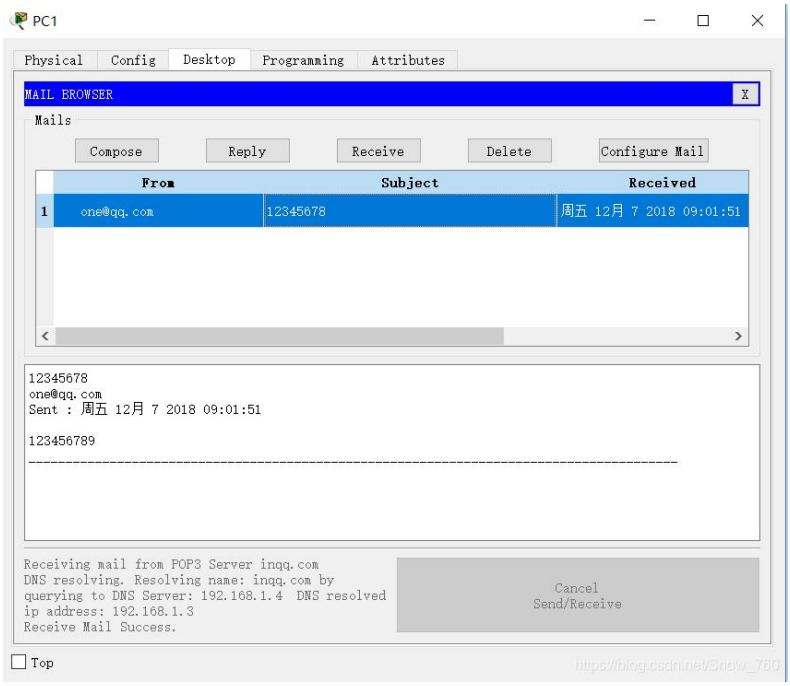
2.3 Smurf 攻击实验
6.1 OSPF 路由项欺骗攻击和防御实验
tips：攻击可以参考 2.4 RIP 路由项欺骗攻击实验
6.2 策略路由项实验

- 中级（0 分~80 分）

2.3 Smurf 攻击实验
6.1 OSPF 路由项欺骗攻击和防御实验
tips：攻击可以参考 2.4 RIP 路由项欺骗攻击实验
6.2 策略路由项实验
6.6 HSRP 实验
7.1 点对点 IP 隧道实验
7.5 ASA5505 SSL VPN 实验
9.1 入侵检测系统实验一

- 高级（0 分~100 分）

2.3 Smurf 攻击实验
6.1 OSPF 路由项欺骗攻击和防御实验
tips：攻击可以参考 2.4 RIP 路由项欺骗攻击实验
6.2 策略路由项实验
6.6 HSRP 实验
7.1 点对点 IP 隧道实验
7.5 ASA5505 SSL VPN 实验
9.1 入侵检测系统实验一
6.3 流量管制实验
tips：对 web 访问的限制，跟钓鱼网站实验有重叠，不做要求。
只要求实现 e-mail 的限制，ui 界面如下所示，可以网上搜索配置教程。



6.4　PAT 实验 、6.5 NAT 实验（二选一）

tips：路由器接口不够，可以参照 P112 6.2.4，使用 NM-2FE2W 增加物理接口数量

开放题：基于 Snort 的入侵检测系统实验（选做，实验说明见本文件最后）

二、提交方式

1．实验报告：每组提交一份，每人负责不同的实验内容，组内不要求必须全部组员都在同一等级；

2．实验验收：每人单独验收，根据自己情况选择难度，并随机回答问题

MOOC 平台上，请以小组形式整体打包提交“pkt 源文件+实验报告书”。在实验报告书内，请注明具体内容或模块的具体成员姓名。将综合考虑整组的完成情况，以及各自负责内容的情况。

三、打分标准

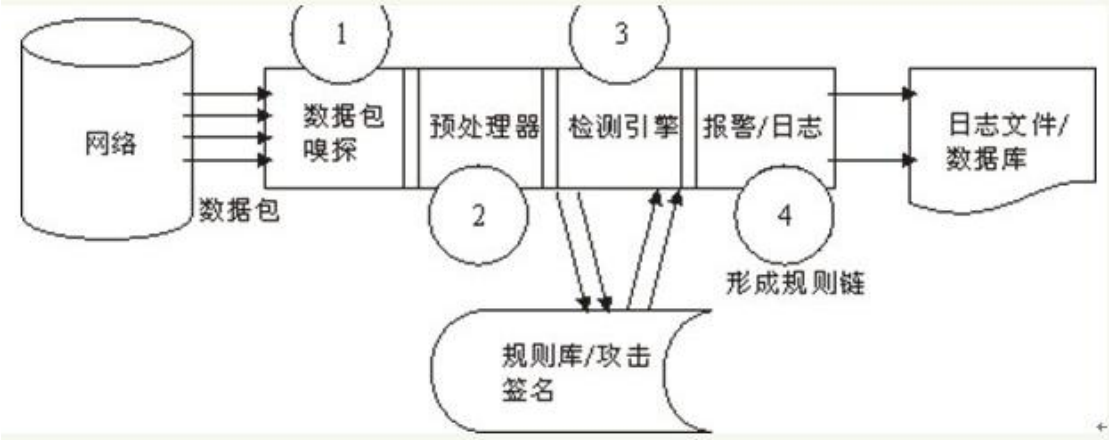
- 完成全部实验并实现全部功能细节；有详细和明确的抓包截图，发现问题和解决问题的思路清晰，详实；文档格式整齐，条理清晰：90-100
- 完成全部实验并实现大部分功能细节；有明确的抓包截图，发现问题和解决问题的思路清晰；文档格式整齐，条理清晰：80-90
- 完成全部实验并实现基本功能细节；有抓包截图但不缺少关键步骤，发现问题和解决问题的思路较清晰；文档格式较整齐，条理较清晰：70-80
- 完成全部实验；有抓包截图不足，发现问题和解决问题的思路清晰；文档格式尚整齐，条理尚清晰：60-70
- 未完成实验；没有抓包截图，没有发现问题和解决问题的思路：60 分以下

Snort 安装及使用

（1）实验原理

Snort 是一个开源的轻量级入侵检测系统（NIDS），使用 C 语言编写，支持 windows、Linux 平台，有三种工作模式，包括：嗅探、记录数据包、入侵检测。嗅探器模式仅仅是从网络上读取数据包并作为连续不断的流显示在终端上。数据包记录器模式把数据包记录到硬盘上。网路入侵检测模式是最复杂的，而且是可配置的。可以让 snort 分析网络数据流以匹配用户定义的一些规则，并根据检测结果采取一定的动作。

Snort IDS 体系结构如图所示。



如上图所示，Snort 的结构由 4 大软件模块组成，它们分别是：

（1）数据包嗅探模块——负责监听网络数据包，对网络进行分析；

（2）预处理模块——该模块用相应的插件来检查原始数据包，从中发现原始数据的“行为”，如端口扫描，IP 碎片等，数据包经过预处理后才传到检测引擎；

（3）检测模块——该模块是 Snort 的核心模块。当数据包从预处理器送过来后，检测引擎依据预先设置的规则检查数据包，一旦发现数据包中的内容和某条规则相匹配，就通知报警模块；

（4）报警/日志模块——经检测引擎检查后的 Snort 数据需要以某种方式输出。如果检测引擎中的某条规则被匹配，则会触发一条报警，这条报警信息会通过网络、UNIXsocket、WindowsPopup(SMB)、SNMP 协议的 trap 命令传送给日志文件，甚至可以将报警传送给第三方插件（如 SnortSam），另外报警信息也可以记入 SQL 数据库。

（2）实验环境

实验主机可以在 windows 下安装，也可以在 linux 下安装 Snort：

- Snort 下载地址（linux 和 windows）：https://www.snort.org/
- windows 环境下，还需要安装 WinPcap，下载地址： https://www.winpcap.org/
- Linux 下安装 Snort 时，根据提示安装其他可依赖包，

参考：https://blog.csdn.net/weixin_43752953/article/details/90748367

- Linux 下使用 Snort 学习链接：

https://blog.csdn.net/weixin_43752953/article/details/90748367

（3）实验任务

- 学习嗅探功能：对网络接口 eth0 进行监听

- 对实验主机的网络接口 eth0 进行监听；
- 实验主机访问 www.hdu.edu.cn；
- 在实验主机上采用详细模式在终端显示数据包网络层、链路层、应用层信息；
- 停止捕获，捕获的数据包存储到日志文件/var/log/snort/snort.log；（存储格式可以是二进制形式，也可以是 ASCII 码形式）

➢ 学习包记录功能：对实验主机网络接口 eth0 进行监听，捕获数据包存储到日志文件中/var/log/snort/snort.log

- 启动 Snort，输入命令，监听主机实验主机的网络接口 eth0，当其他主机 ping 监听主机时，捕获数据包；
- 停止捕获，将捕获的数据包存储到日志文件/var/log/snort/snort.log；（存储格式可以是二进制形式，也可以是 ASCII 码形式）
- 在实验主机上读取 snort.log 文件，查看数据包内容。

➢ 学习入侵检测功能：添加新的规则，当有人通过任何方法以 root 用户身份在计算机外部登录计算机时，该规则将显示警报：

- 在 snort 规则集目录 ids/rules 下新建 snort 规则集文件 new.rules，对来自外部主机的、目标为当前主机的 telnet 数据包进行报警，报警消息自定义；
- 编辑 snort.conf 配置文件，使其包含 new.rules 规则集文件，具体操作如下：使用 vim（或 vi）编辑器打开 snort.conf，切换至编辑模式，在最后添加新行包含规则集文件 new.rules。使用语句 include &RULE PATH/new.rules；
- 以入侵检测方式启动 snort，进行监听，操作命令： snort –c snort.conf ；
- 用外部主机向实验主机主机系统使用 telnet 连接时，验证规则是否有效。

参考：https://www.cnblogs.com/riyir/p/13246607.html

https://www.cnblogs.com/chenguang/p/3742226.html

任务 2：编写代码实现 NIDS 和 HIDS

2.1 基于 Snort 规则实现 NIDS，当有人通过任何方法以 root 用户身份在计算机外部登录计算机时，予以警报，具体过程如下：

➢ 实验的系统环境自选；

➢ 启动抓包工具；

➢ 外部主机使用 telnet 的方式访问实验主机，捕获数据包；

➢ 编写代码，对数据包进行解析，将网络层、链路层、应用层协议字段内容进行提取；

➢ 从 https://www.snort.org/上下载 Snort 规则文件；（文件不能用记事本打开，可以用写字板、notepad++Pycharm 等方式打开）

➢ 基于 Snort 规则对数量中的异常数据包进行检测，并发出告警，告警信息发送到个人邮箱。

2.2 实现 HIDS，具体任务如下：

➢ 实验的系统环境自选；

➢ 显示实验主机中各个应用程序占用内存的情况；

➢ 统计实验主机中各个应用程序一段时间内（10 分钟）使用流量的情况；

➢ 监控某个文件的读写情况；

➢ 显示系统中的启动进程情况；